INTERNET SECURITY SYSTEMS®

INTERNET|SECURITY|SYSTEMS®

proventia® network

Intrusion Prevention System

G and GX Appliances User Guide

IBM Internet Security Systems, Inc.
6303 Barfield Road
Atlanta, Georgia 30328-4233
United States
(404) 236-2600
http://www.iss.net

Copyright © 2003, 2007 IBM Corporation. All rights reserved worldwide.
Customers may make reasonable numbers of copies of this publication for internal use only. This publication may not otherwise be copied or reproduced, in whole or in part, by any other person or entity without the express prior written consent of Internet Security Systems, Inc.

Patent Pending.

Internet Security Systems, ADDME, ActiveAlert, AlertCon, Dynamic Threat Protection, FireCell, FlexCheck, SecurityFusion, SecurePartner, SiteProtector, SecureU, System Scanner, Virtual Patch, Wireless Scanner, and X-Press Update are trademarks and service marks; Database Scanner, Internet Scanner, the Internet Security Systems logo, Online Scanner, Proventia, RealSecure, SAFEsuite, Secure Steps, and X-Force are registered trademarks and service marks of Internet Security Systems, Inc. Network ICE, the Network ICE logo, and ICEpac are trademarks, BlackICE a licensed trademark, and ICEcap a registered trademark of Network ICE Corporation, a wholly owned subsidiary of Internet Security Systems, Inc. Powering Content Security is a trademark and Cobion is a registered trademark of Cobion AG, a wholly owned subsidiary of Internet Security Systems, Inc. SilentRunner is a registered trademark of Raytheon Company. Acrobat and Adobe are registered trademarks of Adobe Systems Incorporated. Certicom is a trademark and Security Builder is a registered trademark of Certicom Corp. Check Point, FireWall-1, OPSEC, Provider-1, and VPN-1 are registered trademarks of Check Point Software Technologies Ltd. or its affiliates. Cisco and Cisco IOS are registered trademarks of Cisco Systems, Inc. HP-UX and OpenView are registered trademarks of Hewlett-Packard Company. IBM and AIX are registered trademarks of IBM Corporation. InstallShield is a registered trademark and service mark of InstallShield Software Corporation in the United States and/or other countries. Intel and Pentium are registered trademarks of Intel. Lucent is a trademark of Lucent Technologies, Inc. ActiveX, Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation. Net8, Oracle, Oracle8, SQL*Loader, and SQL*Plus are trademarks or registered trademarks of Oracle Corporation. Seagate Crystal Reports, Seagate Info, Seagate, Seagate Software, and the Seagate logo are trademarks or registered trademarks of Seagate Software Holdings, Inc. and/or Seagate Technology, Inc. Secure Shell and SSH are trademarks or registered trademarks of SSH Communications Security. iplanet, Sun, Sun Microsystems, the Sun Logo, Netra, SHIELD, Solaris, SPARC, and UltraSPARC are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Adaptive Server, SQL, SQL Server, and Sybase are trademarks of Sybase, Inc., its affiliates and licensers. Tivoli is a registered trademark of Tivoli Systems Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd. All other trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications are subject to change without notice.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than ISS or the X-Force. Use of this information constitutes acceptance for use in an "AS IS" condition, without warranties of any kind, and any use of this information is at the user's own risk. ISS and the X-Force disclaim all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall ISS or the X-Force be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if ISS or the X-Force has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Internet Security Systems, Inc. The views and opinions of authors expressed herein do not necessarily state or reflect those of Internet Security Systems, Inc., and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents Internet Security Systems from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to support@iss.net.

August 8, 2007

Contents

Preface . . . 7
Overview . . . 7
About Proventia Appliance Documentation . . . 8
Conventions Used in this Guide . . . 9
Getting Technical Support . . . 10
. . . 12

Chapter 1: Introducing the Proventia Network Intrusion Prevention System . . . 13
Overview . . . 13
Intrusion Prevention . . . 14
Management Features . . . 16
Appliance Adapter Modes . . . 17
High Availability Modes . . . 18

Chapter 2: Configuring Appliance Settings . . . 19
Overview . . . 19
Configuration Settings Checklist . . . 20
Using Proventia Setup . . . 21
Configuring Other Appliance Settings . . . 24
Reinstalling Appliance Firmware . . . 28

Chapter 3: Configuring Appliances for High Availability . . . 33
Overview . . . 33
About High Availability . . . 34
High Availability Configuration Overview . . . 36
High Availability Deployment . . . 37

Chapter 4: Using Proventia Manager . . . 39
Overview . . . 39
Completing the Configuration . . . 40
Accessing Proventia Manager . . . 42
Navigating Proventia Manager . . . 43
Installing the License File . . . 46
Working with Proventia Manager . . . 47

Chapter 5: Updating the Appliance . . . 49
Overview . . . 49
Updating the Appliance . . . 50
Updating the Appliance Automatically . . . 52
Updating the Appliance Manually . . . 54
Using Update Tools . . . 55
Using Advanced Parameters to Tune Update Settings . . . 56

Chapter 6: Managing the Appliance through SiteProtector . . . 59
Overview . . . 59
Managing with SiteProtector . . . 60
Configuring SiteProtector Management . . . 62
Navigating SiteProtector . . . 65

Chapter 7: Configuring Responses . . . 67
Overview . . . 67
About Responses . . . 68
Configuring Email Responses . . . 69
Configuring the Log Evidence Response . . . 71
Configuring Quarantine Responses . . . 72
Configuring SNMP Responses . . . 73
Configuring User Specified Responses . . . 75

Chapter 8: Working with Security Events . . . 77
Overview . . . 77
Configuring Protection Domains . . . 78
Configuring Security Events . . . 80
Assigning Multiple Security Events to a Protection Domain . . . 83
Viewing Security Event Information . . . 84
Configuring Response Filters . . . 86
Viewing Response Filter Information . . . 90

Chapter 9: Configuring Other Intrusion Prevention Settings . . . 91
Overview . . . 91
Managing Quarantined Intrusions . . . 92
Configuring Connection Events . . . 93
Configuring User-Defined Events . . . 97
User-Defined Event Contexts . . . 100
Regular Expressions in User-Defined Events . . . 105
Viewing User Defined Event Information . . . 107
Configuring OpenSignature . . . 108
Configuring Global Tuning Parameters . . . 110
Configuring X-Force Default Blocking . . . 112

Chapter 10: Configuring Firewall Settings . . . 113
Overview . . . 113
Configuring Firewall Rules . . . 114
Firewall Rules Language . . . 117
Tuning Firewall Logging . . . 120

Chapter 11: Configuring Local Tuning Parameters . . . 121
Overview . . . 121
Configuring Alerts . . . 122
Managing Network Adapter Cards . . . 125
Managing the Alert Queue . . . 128
Configuring Advanced Parameters . . . 129
Configuring TCPReset . . . 133
Increasing Maximum Network Frame Size . . . 134

Chapter 12: Managing System Settings . . . 135
Overview . . . 135
Viewing System Status . . . 136
Managing Log Files . . . 137
Working with System Tools . . . 138
Configuring User Access . . . 139
Installing and Viewing Current Licenses . . . 140

Chapter 13: Viewing Alerts and System Information 141
Viewing Alerts 142
Managing Saved Alert Files 145
Viewing Notifications Status 146
Viewing Statistics. 147

Index 149

Preface

Overview

Purpose

This guide is designed to help you create and maintain policies for your Proventia Network IPS G and GX appliances. It also explains how to manage these appliances using Proventia Manager software.

Scope

This guide describes the features in Proventia Manager and explains how to configure the appliance, configure policy settings, and manage the appliance.

Audience

This guide is intended for network security system administrators responsible for setting up, configuring and managing the Proventia Network IPS in a network environment. A fundamental knowledge of network security policies and IP network configuration is helpful.

Supported appliance models

This Proventia Network IPS firmware update supports the following G and GX models:

- Proventia G 100/200/400/1000/1200/2000 running Firmware Update 1.2
- Proventia GX3002
- Proventia GX4002 and GX4004
- Proventia GX5008 (C and CF) and GX5108 (C and CF)
- Proventia GX6116

SiteProtector support

This Proventia Network IPS release supports appliance management with the following SiteProtector versions:

- SiteProtector 2.0 Service Pack 6.0
- SiteProtector 2.0 Service Pack 6.1

Important: The Proventia Network IPS GX6116 appliance supports **only** SiteProtector 2.0 Service Pack 6.1.

About Proventia Appliance Documentation

Introduction

This guide explains how to configure intrusion prevention, firewall settings, and other policy settings for the Proventia Network IPS appliances using Proventia Manager, the local management interface. It also provides information for managing the appliances using both the Proventia Configuration Menu and Proventia Manager.

Locating additional documentation

Additional documentation described in this topic is available on the ISS Web site at http://www.iss.net/support/documentation/.

Related publications

See the following for more information about the appliance:

Document	Contents
Proventia Network Intrusion Prevention System Help	Help located in Proventia Manager and the Proventia Network IPS Policy Editor in SiteProtector.
Proventia Network Intrusion Prevention System Data Sheet	General information about previous Proventia Network IPS (formerly G Series) appliance features.
Proventia Network Intrusion Prevention System Frequently Asked Questions	Frequently asked questions about the appliance and its functions.
Readme File	The most current information about product issues and updates, and how to contact Technical Support located at http://www.iss.net/download/.

Table 1: *Reference documentation*

Knowledgebase

The IBM ISS support knowledgebase is a valuable source of information. Visit the knowledgebase at http://www.iss.net/support/knowledgebase/. You can search the knowledgebase using key works or Answer IDs.

Tip: See Answer ID 3321 for the latest tips and known issues for Proventia Network Intrusion Prevention System appliances.

Conventions Used in this Guide

Introduction

This topic explains the typographic conventions used in this guide to make information in procedures and commands easier to recognize.

In procedures

The typographic conventions used in procedures are shown in the following table:

Convention	What it Indicates	Examples
Bold	An element on the graphical user interface.	Type the computer's address in the **IP Address** box. Select the **Print** check box. Click **OK**.
SMALL CAPS	A key on the keyboard.	Press ENTER. Press the PLUS SIGN (+).
`Constant width`	A file name, folder name, path name, or other information that you must type exactly as shown.	Save the `User.txt` file in the `Addresses` folder. Type `IUSR__SMA` in the **Username** box.
`Constant width italic`	A file name, folder name, path name, or other information that you must supply.	Type `Version` *`number`* in the **Identification information** box.
→	A sequence of commands from the taskbar or menu bar.	From the taskbar, select **Start→Run**. On the **File** menu, select **Utilities→Compare Documents.**

Table 2: *Typographic conventions for procedures*

Command conventions

The typographic conventions used for command lines are shown in the following table:

Convention	What it Indicates	Examples
`Constant width bold`	Information to type in exactly as shown.	**`md ISS`**
`Italic`	Information that varies according to your circumstances.	**`md`** *`your_folder_name`*
[ ]	Optional information.	**`dir`** [*`drive:`*] [*`path`*] [*`filename`*] [**`/P`**] [**`/W`**] [**`/D`**]
|	Two mutually exclusive choices.	**`verify`** [**`ON`**|**`OFF`**]
{ }	A set of choices from which you must choose one.	**`% chmod`** {**`u g o a`**}=[**`r`**] [**`w`**] [**`x`**] *`file`*

Table 3: *Typographic conventions for commands*

Getting Technical Support

Introduction

ISS provides technical support through its Web site and by email or telephone.

The ISS Web site

The Internet Security Systems (ISS) Resource Center Web site (http://www.iss.net/support/) provides direct access to frequently asked questions (FAQs), white papers, online user documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase (http://www.iss.net/support/knowledgebase/).

Support levels

ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24-7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 4: *Hours for technical support*

Contact information

The following table provides electronic support information and telephone numbers for technical support requests:

Regional Office	Electronic Support	Telephone Number
North America	Connect to the MYISS section of our Web site: www.iss.net	**Standard:** (1) (888) 447-4861 (toll free) (1) (404) 236-2700 **Select and Premium:** Refer to your Welcome Kit or call your Primary Designated Contact for this information.
Latin America	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700

Table 5: *Contact information for technical support*

Regional Office	Electronic Support	Telephone Number
Europe, Middle East, and Africa	support@iss.net	(44) (1753) 845105
Asia-Pacific, Australia, and the Philippines	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Japan	support@isskk.co.jp	Domestic: (81) (3) 5740-4065

Table 5: *Contact information for technical support (Continued)*

Chapter 1

Introducing the Proventia Network Intrusion Prevention System

Overview

Introduction

This chapter introduces the Proventia Network Intrusion Prevention System (IPS) and describes how its features protect the network with a minimum of configuration. It also describes other Proventia Network IPS features you can implement to customize your network's security.

In this chapter

This chapter contains the following topics:

Topic	Page
Intrusion Prevention	14
Management Features	16
Appliance Adapter Modes	17
High Availability Modes	18

Intrusion Prevention

Introduction

The Proventia Network Intrusion Prevention System (IPS) automatically blocks malicious attacks while preserving network bandwidth and availability. The Proventia Network IPS appliances are purpose-built, Layer 2 network security appliances that you can deploy either at the gateway or the network to block intrusion attempts, denial of service (DoS) attacks, malicious code, backdoors, spyware, peer-to-peer applications, and a growing list of threats without requiring extensive network reconfiguration.

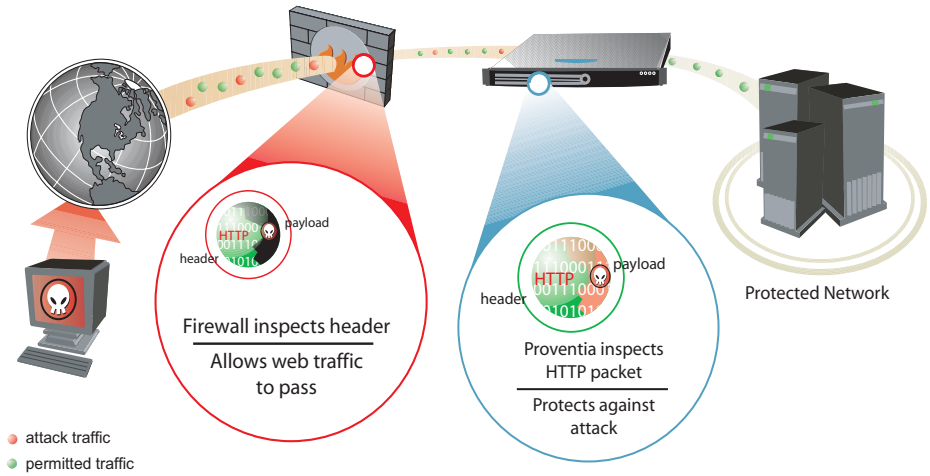

Figure 1: *Intrusion prevention overview*

Figure 1 illustrates how the Proventia Network IPS protects your network. With flexible deployment options and out-of-the-box functionality, these appliances ensure accurate, high-performance protection at both the network perimeter and across internal networks and internal network segments.

Protection features

Proventia intrusion prevention features include proven detection and prevention technologies, along with the latest security updates. These appliances understand the logical flow and state of traffic, resulting in unsurpassed protection against network threats, including trojans, backdoors and worms.

Proventia Network IPS offers the following features to protect your network against threats:

- **Dynamic blocking**

  Proventia Network IPS uses vulnerability-based attack identification to enable an immediate and reliable blocking response to unwanted traffic while allowing legitimate traffic to pass unhindered. It employs a deep traffic inspection process that uses detection-based blocking to stop both known attacks and previously unknown attacks.

- **Firewall rules**

  You can create firewall rules that enable the appliance to block incoming packets from particular IP addresses, port numbers, protocols, or VLANs. These rules block many attacks before they affect your network.

- **Automatic security content updates based on the latest security research**

  You can automatically download and activate updated security content. The security updates you receive are a result of ISS's X-Force Research and Development Team's ongoing commitment to provide the most up-to-date protection against known and unknown threats.

- **Quarantine and block responses**

  Inline appliances use the quarantine response to block traffic for a specified amount of time after an initial attack, and they use the block response to block and reset a connection in which an event occurs or to drop the packet that triggered an event.

- **Virtual Patch™ protection**

  Proventia's Virtual Patch capability provides a valuable time buffer, eliminating the need for you to immediately patch all vulnerable systems. You can wait until you are ready to manually update appliances or until scheduled updates occur, rather than having to patch and restart systems.

- **SNMP support**

  Using SNMP-based traps, you can monitor key system problem indicators or respond to security or other appliance events using SNMP responses.

Management Features

Overview

You can create and deploy security policies, manage alerts, and apply updates for your appliances either locally or through a central appliance management system.

Proventia Network IPS offers you the following tools for managing appliances:

- Proventia Configuration Menu
- Proventia Manager
- SiteProtector

Proventia Configuration Menu

The Proventia Configuration Menu is the local configuration interface you use to configure your appliance settings.

Proventia Manager

Proventia Manager offers a browser-based graphical user interface (GUI) for local, single appliance management. You can use Proventia Manager to manage the following functions:

- monitoring appliance's status
- configuring operation modes
- configuring firewall settings
- managing appliance settings and activities
- reviewing alert details
- configuring high availability
- managing security policies with protection domains.

SiteProtector

SiteProtector is the ISS central management console. With SiteProtector, you can manage components and appliances, monitor events, and schedule reports. By default, your appliance is set up to be managed through Proventia Manager. If you are managing a group of appliances along with other sensors, you may prefer the centralized management capabilities that SiteProtector provides.

When you register your appliance with SiteProtector, SiteProtector controls the following management functions of the appliance:

- Firewall settings
- Intrusion prevention settings
- Alert events
- Appliance and security content updates

After you register the appliance with SiteProtector, you can *view* these functions in Proventia Manager but you can *change* them only from SiteProtector.

Reference: For instructions on managing the appliance through SiteProtector, see the SiteProtector user documentation at http://www.iss.net/support/documentation/ or the SiteProtector Help.

Appliance Adapter Modes

Introduction

The inline appliances include three adapter modes as follows:

- inline protection
- inline simulation
- passive monitoring

You selected one of these operation modes when you configured the appliance settings. Using the Proventia Configuration menu, if you like, you can use the default operation mode and select a different one later.

Adapter modes

Inline Protection

This mode allows you to fully integrate the appliance into the network infrastructure. In addition to the block and quarantine responses, all firewall rules are enabled, and the full security policy you apply to the appliance is enabled.

Inline Simulation

This mode allows you to monitor the network using the appliance without affecting traffic patterns. In addition to the traditional Block response, the appliance also uses the Quarantine response. Packets are not dropped when these responses are invoked, and the appliance does not reset TCP connections by default. This mode is helpful for baselining and testing your security policy without affecting network traffic.

Passive Monitoring

This mode replicates traditional passive intrusion detection system (IDS) functionality, monitoring network traffic without sitting inline. It mainly responds to intrusions with a traditional block response. If the appliance encounters suspicious network activity, it sends a reset to block a TCP connection. This mode is helpful for determining what type of inline protection your network requires.

Changing appliance adapter modes

If you change between the passive monitoring mode and the inline simulation or inline protection mode, you must also change the network connections to your appliance. An appliance operating in passive monitoring mode requires a connection to a tap, hub, or SPAN port.

If you change the appliance adapter mode from inline simulation to inline protection, you may need to modify some advanced parameters to set them appropriately for inline protection. See “Editing network adapter card properties” on page 125 for more information.

High Availability Modes

Introduction

The Proventia Network IPS High Availability (HA) feature enables appliances to work in an *existing* high availability network environment. The appliances pass all traffic between them over mirroring links, ensuring that both appliances see all of the traffic over the network and thus maintain state. This approach also allows the appliances to see asymmetrically routed traffic in order to fully protect the network.

High Availability support is limited to two cooperating appliances. Both appliances process packets inline, block attack traffic that arrives on their inline protection ports, and report events received on their inline ports to the management console.

HA models

You can use the following appliance models in an existing HA environment:

- G400 series appliances
- G2000 series appliances
- GX5000 series appliances
- GX6000 series appliances

Important: You cannot *mix* models in a single HA environment. For example, you cannot use a G2000 appliance and a GX5008 appliance as an HA pair.

About HA modes

You can select one of the following modes for an HA-capable appliance:

- normal mode
- HA protection mode
- HA simulation mode

Normal mode

In Normal operation mode, the appliance cannot operate with another appliance in HA mode. Appliances can be configured to run in inline protection, inline simulation, and passive monitoring modes at the adapter level only.

HA protection mode

In protection mode, both HA partner appliances monitor traffic inline. Each appliance reports and blocks the attacks received on its inline ports. The appliances also monitor the traffic on each other's segments using mirror links, ready to take over reporting and protection in case of network failover.

HA simulation mode

In HA simulation mode, both HA partner appliances monitor traffic inline, but do not block any traffic. Instead they provide passive notification responses. The appliances also monitor the traffic on each other's segments using mirror links, ready to take over notification in case of network failover.

Chapter 2

Configuring Appliance Settings

Overview

Introduction

This chapter describes how to use Proventia Setup to connect the Proventia Network IPS appliance to the network. It also outlines other appliance settings you can configure at any time, such as backup and restore settings and SNMP settings.

In this chapter

This chapter contains the following:

Topic	Page
Configuration Settings Checklist	20
Using Proventia Setup	21
Configuring Other Appliance Settings	24
Reinstalling Appliance Firmware	28

Configuration Settings Checklist

Introduction

Using Proventia Setup, you can configure basic network settings, as well as passwords, DNS and host name, adapter modes, port link settings, the date and time, backup and recovery settings, and SNMP configuration. You need to gather some relevant information before you begin.

Checklist

Use the checklist to obtain the information you need to configure the Proventia Network IPS appliance.

✓	Setting	Description
❑	Hostname	The unique computer name for the appliance **Example:** *myappliance*
	Your setting:	
❑	Domain name	The domain suffix for the network **Example:** *mydomain.com*
	Your setting:	
❑	Domain name server	The server IP address for domain name lookups (DNS search path). (optional).
	Your setting:	
❑	Management Port IP Address	An IP address for the management network adapter.
	Your setting:	
❑	Management port subnet mask	The subnet mask value for the network connected to the management port
	Your setting:	
❑	Management port default gateway (IP address)	The IP address for the management gateway
	Your setting:	
❑	Adapter mode	The adapter mode to use for the appliance **Note**: The adapter mode you plan to use should correspond to the way you connected the network cables.
	Your setting:	

Table 6: *Checklist for configuration information*

Using Proventia Setup

Introduction

If you want to configure the appliance from a computer, follow the procedure below, which explains how to connect to the appliance using Hyperterminal. Follow the instructions listed in the documentation for your program.

Establishing a serial connection to the appliance

To connect to the appliance using Hyperterminal:

1. On your computer, select **Start→ Programs→ Accessories→ Communications.**
2. Select **Hyperterminal**.
3. Create a new connection using the following settings:

Setting	Value
Communications Port	Typically COM1 (depending on computer setup)
Emulation	VT100
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

4. Press ENTER to establish a connection.

   When the connection is established, the login screen appears.

   Tip: If you are unable to establish a connection, make sure that the appliance has power and that you have started the appliance.

Caution for GX6000-series appliances

Do not turn the appliance off or remove power from the appliance at any time during the installation process. Removing power can corrupt the installation process and permanently damage the appliance, resulting in a situation whereby the appliance must be returned to the factory.

If you want to turn the appliance off, wait until *after* you see the unconfigured login prompt.

Completing the initial configuration

To complete the initial configuration for the appliance:

1. At the unconfigured login prompt, type the user name **`admin`**, and then press ENTER.
2. To enter the password, type the default password **`admin`**.

   Note: If you configured initial network settings for your GX4000, GX5000, or GX6000 series appliance using the LCD panel, type the case-sensitive password the appliance generated for you.
3. Select **Start**, and then press ENTER.
4. Read the Software License Agreement, and then select **Accept** to continue.

5. Follow the on-screen instructions.

   The following table describes the required information.

Information	Description
Change Password	• **Admin Password**—When you access the appliance, you must provide this password. This password can be the same as the root password. • **Root Password**—When you access the appliance from a command line, you must provide this password. • **Proventia Manager Password**—When you access Proventia Manager, the appliance's Web interface, you must provide this password. This password can be the same as the root password.
Network Configuration Information	• **IP Address**—The IP address of the management network adapter. • **Subnet Mask**—The subnet mask value for the network that connects to the management interface. • **Default Gateway**—The IP address for the management gateway. **Note**: If you initially configured the appliance through the LCD panel, the information you entered appears here. You can change this information as needed.
Host Configuration	The appliance uses domain names and DNS information to send email and SNMP responses. If you do not configure this information during setup, you must specify the IP address of the appliance's mail server each time you define an email or SNMP response. • **Hostname**—The computer name for the appliance. Example: myappliance. • **Domain Name**—The domain suffix (DNS search path) for the network. Example: mycompany.com. • **Primary Name Server**—The IP address for the DNS used to perform domain name lookups. • **Secondary Name Server**—The IP address for the secondary DNS used to perform domain name lookups.
Time Zone Configuration	These settings determine the time zone for the appliance.
Date/Time Configuration	You must set the date and time for the appliance as it appears in the management interface, so you can accurately track events as they occur on the network.
Agent Name Configuration	The Agent Name is the appliance name as it appears in the management interface. This name should correspond to a meaningful classification in the network scheme, such as the appliance's geographic location, business unit, or building address.

Information	Description
Port Link Configuration	Port link settings determine the appliance's performance mode, or how the appliance handles its connection to the network. You can select the speed (the rate at which traffic passes between the appliance and the network) and the duplex mode (which direction the information flows). Select link speeds and settings compatible with your particular network and in relation to the other devices that bracket the Proventia Network IPS appliance. If you are not sure about your network settings, select Auto to enable the appliance to negotiate the speed and duplex mode with the network automatically.
Adapter Mode Configuration	The Adapter Mode determines how the appliance behaves within the network in order to protect it. Review "Appliance Adapter Modes" on page 17 if you are not sure which mode to select. You can select different adapter modes for each port pair, but you must confirm that you have selected the correct adapter mode for the appliance's physical network connections. You may experience significant network implications if you have configured this setting incorrectly. **Note**: If you plan to run two appliances in High Availability mode, you must select an adapter mode during the initial setup. After you complete the initial configuration, you can set the corresponding HA mode through the management interface. See "Configuring Appliances for High Availability" on page 33 for more information.

When you have entered all the information, the appliance applies the settings.

6. When you are prompted, press ENTER to log off the appliance.

Configuring Other Appliance Settings

Introduction

Through the Configuration Menu, you can view or edit the appliance settings that you configured during the initial setup. You can also manage the following important appliance settings:

Select this menu option...	To do this...
Appliance Information	View information about the appliance.
Appliance Management	• Back up the current configuration. • Restore current configuration or factory default. • Disable remote root access to the appliance. • Restart or shut down the appliance.
Agent Management	• View the version or status information for the Agent, Engine, or Daemon. • Change the agent name.
Network Configuration	• Change the IP address, subnet mask, or gateway. • Change the host name, domain name, or the primary and secondary DNS. • Change management port link settings. • Specify kill port link settings.
Time Configuration	• Change the time zone, date, or time for the appliance. • Configure the network time protocol.
Password Management	Change the admin, root, or Proventia Manager passwords.
SNMP Configuration	Enable the appliance to send SNMP traps when appliance system-related events occur.

Table 7: *Configuration Menu*

Appliance information

You can view the following information about appliance settings:

Item	Description
Serial Number	The appliance's serial number.
Base Version	The firmware version with which the appliance was shipped from the factory.
XPU Version	The latest X-Press Update (XPU) or security content update version installed on the appliance.
Firmware Version	The latest firmware version installed on the appliance.
Agent Name	The appliance's model name, such as Proventia_GX6116.
Host Name	The name given to the appliance when it was installed, as it appears on the network. This name appears in the management interface.
IP Address	The IP address you use to manage the appliance through Proventia Manager and SiteProtector.

Table 8: *Appliance information*

Item	Description
Netmask	The subnet mask value for the network that connects to the management port.
Gateway	The IP address for the management gateway.
Primary DNS	The IP address of the primary server you use to perform domain name lookups (DNS search path).
Secondary DNS	The IP address of the secondary server you use to perform domain name lookups (DNS search path).

Table 8: *Appliance information (Continued)*

Appliance management

From the Appliance Management Menu, you can perform the following tasks:

Task	Description
Back up the current configuration	When you back up the current configuration, all custom information is saved to an image file that resides on a special backup partition on the appliance's hard drive. When you restore an image from the current backup file, the hard drive is re-imaged with the information you have saved, and everything is overwritten except the special backup partition.
Restore the configuration	You have two options for restoring the configuration: • **Backup configuration**—Restores the appliance settings to the most current backup configuration. • **Factory default**— Restores the appliance settings to the factory default firmware version. **Note**: This option preserves the current host, network, time zone, and password settings.
Disable remote root access	You can disable remote access to the root user. If you disable remote access, the root user can only log on to the appliance from a local console. After you disable access, only the admin user has remote access permission. You can re-enable remote root access by logging into the appliance as the root user through a terminal emulation session, and then typing `enable-root-access` at the command prompt.
Reboot or shut down the appliance	You can also reboot or shut down the appliance from the LCD panel or Proventia Manager.

Table 9: *Appliance management tasks*

Agent management

From the Agent Management Menu, you can perform the following tasks:

Task	Description
View the agent status	You can view the agent, engine, and daemon status.
Change the agent name	The agent name is the appliance name that appears in the management console, either Proventia Manager or SiteProtector. If you change the agent name, the new name appears in SiteProtector after the next heartbeat.

Table 10: *Agent management tasks*

Network configuration

From the Network Configuration Menu, you can perform the following tasks:

Task	Description
Change IP Settings	You can change the IP address, subnet mask, or gateway for the appliance. For example, you might need to change these settings if you moved the appliance to a different location or network area.
Change host name settings	You can change the hostname, domain name, and primary and secondary name servers for the appliance. For example, you might change these settings if you add a new email server or SNMP management console, because appliances uses domain names and DNS information to send Email and SNMP responses.
Change management port link settings	You can change the link speed and duplex settings for the management port. Select link speeds and duplex settings compatible with your particular network and in relation to the other devices that bracket the Proventia Network IPS appliance.
Specify TCPReset (kill) port link settings	When you connect the TCPReset (kill) port, you can change the link and duplex settings here. See “Configuring TCPReset” on page 133 for information about initial setup for kill ports.

Table 11: *Network configuration tasks*

Time configuration

From the Time Configuration Menu, you can perform the following tasks:

Task	Description
Change the date and time	The time and date you set for the appliance determines when appliance events are recorded and how they appear in the management interface.
Change the time zone	Ensure you have the correct time zone set for the appliance. After you set this value, you should not have to change it unless you physically relocate the appliance.
Set the network time protocol	The network time protocol (NTP) synchronizes the local date and time with the network time server. If you specify more than one time server, the appliance gets a number of samples from each server you specify to determine the correct time.

Table 12: *Time configuration tasks*

Password management

From the Password Management Menu, you can perform the following tasks:

Task	Description
Change admin, root, or Proventia Manager passwords	You can use Proventia Manager to also change passwords. See “Configuring User Access” on page 139.
Disable the boot loader password	The boot loader password protects the appliance from unauthorized user access during the boot process. When you set a root password, the boot loader password is automatically enabled and set to the same password. You can disable the boot loader password; the root password remains active.

Table 13: *Password management tasks*

SNMP configuration

When you enable SNMP from the Configuration Menu, you are enabling the appliance to send information about system health-related events such as low disk space, low swap space, very high CPU usage, or physical intrusions. These settings do not affect SNMP responses assigned to events that occur on the network. For information about SNMP responses to events, see “Configuring SNMP Responses” on page 73.

From the SNMP Configuration Menu, you can perform the following tasks:

Task	Description
Enable SNMP	Guides you through providing the information the appliance needs to communicate with the SNMP manager. You provide the following information: • System location, contact, and name • IP address for the main trap receiver • Communication port number (port 162 by default) • Community string (public or private) • Trap version
Disable SNMP	Stops the appliance from sending system related information to the SNMP manager and removes all previous configurations.
Start or stop the SNMP daemon	Allows you to restart or temporarily disable the SNMP service.
View SNMP system information	View the current SNMP settings for the appliance.
Add or delete a trap receiver	The trap receiver IP address is the server address where the SNMP Manager is running. The SNMP Host must be accessible to the appliance to send SNMP traps. Allows you to add additional trap receivers to receive messages from the appliance, or to delete a trap receiver you no longer want to receive messages.
Enable read access for the trap receiver	Allows the SNMP Manager to collect information about system-related events. **Important**: If you choose to allow SNMP read access, UDP port 161 is opened on the appliance firewall.

Table 14: *SNMP configuration tasks*

Reinstalling Appliance Firmware

Introduction

The Recovery CD included in the appliance packaging contains the software that was installed on the appliance at the factory. You can reinstall the software from this CD on the appliance.

Results

This process does the following:

- Overwrites software configuration changes you have made since you first installed the appliance.
- Restores the original, default login credentials:
  - username = admin
  - password = admin

Supported network cards

If your appliance does not have an internal CD drive, you must use a separate computer to reinstall the firmware. The computer you use must have one of the following network cards installed for you to complete the reinstallation successfully:

Important: ISS supports only the network cards listed.

Card	Brand Manufacturer
e1000	Intel PRO/1000
e100	Intel PRO/100
3c59x	3Com 3c590, 3c595, 3c905, 3c575
bcm5700	Broadcom 57xx Gigabit
sk98lin	SysKonnect and Marvell Gigabit
tulip	Digital/Intel 21x4x “Tulip”
eepro100	Intel PRO/100
8139too	RealTek 8139
ne2k-pci	NE2000-compatible PCI cards
pcnet32	AMD PCnet32, VMWare
sis900	SiS 900, 7016
via-rhine	Via Rhine VT86C100A, 6102, 6105
8139cp	RealTek 8139C+
epic100	SMC83c170, SMC83c175
xircom_cb	Xircom CardBus
3c574_cs	3Com 3c574
axnet_cs	Asix AX88190
nmclan_cs	AMD Am79C940

Table 15: *Supported network cards*

Card	Brand Manufacturer
smc91c92_cs	SMC 91c92
xirc2ps_cs	Xircom CE2, CE IIps, RE-10, CEM28, CEM33, CEM56, CE3-100, CE3B, RE-100, REM10BT, REM56G-100
3c589_cs	3Com 3c589
fmvjl8x_cs	FMV J181, FMV J182, TDK LAK-CD021, ConTec C-NET (PC) C, Ungermann Access/CARD
pcnet_cs/NE2000 compatible cards	D-Link DE-650, Linksys PCMCIA, Accton EN2212, RPTI EP400, PreMax PE-200, IBM Credit Card Adapter, Novell NE4100, Kingston KNE-PCM/x, Allied Telesis LA-PCM, ASANTE FriendlyNet

Table 15: *Supported network cards*

Preparing to reinstall firmware

Before you reinstall the appliance firmware, complete the following tasks:

✓	Description
❑	Choose a computer to access the appliance and reinstall the software. This computer is referred to as the *Pre-boot eXecution (PXE) server*. **Requirements:** • The BIOS settings on the computer must allow it to restart from a CD. For more information, see the computer's documentation. • Pentium II or compatible CPU • 64M RAM • IDE CD-ROM drive • COM1 serial port
❑	Locate the following items included with the appliance package: • *Proventia Network Intrusion Prevention System Recovery CD* • an Ethernet cross-over cable • a serial (null modem) cable **Note:** ISS does not support the use of other cables.
❑	Record the following appliance settings for the management interface: • IP address, subnet mask, and default gateway • hostname, domain name, and DNS name server

Table 16: *Before you reinstall the appliance firmware*

✓	Description
❑	Turn off the appliance, and then connect the computer (PXE server) directly to the appliance with the provided cables. See diagram below. **Connect the null modem cable to the devices as follows:** • On the computer (PXE server), use the port labeled COM1. • On the appliance, use the port labeled **Console**. **Connect the Ethernet cable to the devices as follows:** • On the computer (PXE server), use the Ethernet port. • On the appliance, use the left **Management** port labeled **1**. **Note:** Connecting to the computer (PXE server) to the appliance disables the appliance-Internet connection. When you finish the reinstall process, you must re-establish the Internet connection to retrieve appliance updates. **Important**: If you are running multiple PXE servers on the network, then you need to disconnect them prior to running the Proventia Network IPS reinstallation. You can verify that you are accessing the correct PXE server by the message displayed in Step 5.

Table 16: *Before you reinstall the appliance firmware (Continued)*

Caution for GX6000-series appliances

Do not turn the appliance off or remove power from the appliance at any time during the reinstallation process. Removing power can corrupt the installation process and permanently damage the appliance, resulting in a situation whereby the appliance must be returned to the factory.

If you want to turn the appliance off, wait until *after* you see the unconfigured login prompt.

Reinstalling the appliance software using a PXE boot server

To reinstall the appliance software:

1. Turn the appliance off.
2. Insert the *Proventia Network Intrusion Prevention System Recovery CD* into the CD-ROM drive of the PXE boot server, and then restart the PXE boot server.
3. If you are prompted to do so, type **`bootserv`** and press ENTER.

   The PXE boot server displays the following messages:

   ```
   ***You may now boot your Proventia GXxxxx via the network***
   ***Starting Terminal Emulator***
   ***Press Control-G to Exit and Reboot***
   ```

   Note: The PXE boot server now acts as a terminal emulator for the appliance and displays the console output of the appliance.
4. Turn on the appliance.

   The PXE boot server displays boot process messages, and then displays the following prompt:

   ```
   Press L to boot from LAN, or press any other key to boot normally.
   ```

   Important: The installation process allows only five (5) seconds for you press L to boot from LAN. If you do not press L within this time period, the appliance boots as usual, and you must restart the appliance.

5. Press the L key.

   The following message appears:

   ```
   Internet Security Systems
   Proventia GXxxxx Recovery Boot
   ```

   The PXE boot server displays status messages from the appliance, and then boots the installer over the network.

6. At the prompt, type **`reinstall`**, and then press ENTER.

   The installer reloads the operating system.

   Note: When the reinstallation is complete, the appliance automatically reboots. Let the appliance complete the boot process without interruption.

7. When the appliance has rebooted, the `unconfigured.appliance login` prompt appears.

   You can log in with the default user and password of admin/admin and configure the appliance using the Configuration Menu, or you can configure the appliance using the LCD panel on the front of the appliance.

Reinstalling using a USB CD-ROM drive

To reinstall an appliance using a USB CD-ROM drive:

1. Turn the appliance off.
2. Connect a USB CD-ROM drive to the USB port on the appliance.
3. Connect one end of the serial console cable to the console port of the appliance and connect the other end to the serial port on another computer.
4. Establish a serial connection from the computer to the appliance using a terminal emulation program. Use the following settings:
   - Port: The serial port you have used on the computer, usually COM1.
   - Emulation: VT100
   - Bits per second: 9600
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None
5. Restart the appliance and insert the recovery CD into the USB CD-ROM drive.
6. The appliance starts up from the CD and displays the following message:

   ```
   CAUTION: Reinstalling from the recovery CD restores the appliance to
   its original configuration and removes any customized settings. The
   appliance also reverts to the default password.
   ```

7. Type “reinstall,” and press ENTER.
   When the reinstallation process is complete, the appliance automatically restarts.

   IMPORTANT: Let the appliance complete the boot process without interruption. Otherwise, you could risk damaging the appliance.

Reconfiguring the appliance

To reconfigure the appliance after you reinstall the software, follow the setup instructions in "Using Proventia Setup" on page 21.

Notes:

- You should complete the appliance configuration while connected to the PXE boot server. When you have completed all reinstallation and reconfiguration steps, press CTRL+G to shut down the PXE server.
- To access firmware and database updates, you must have Internet access. Disconnect the PXE boot server and re-connect the management interface to the network for Internet access.

Chapter 3

Configuring Appliances for High Availability

Overview

Introduction

This chapter explains how to configure HA- capable models to work in an existing high availability network environment.

In this chapter

This chapter contains the following topics:

Topic	Page
About High Availability	34
High Availability Configuration Overview	36
High Availability Deployment	37

About High Availability

Introduction

The Proventia Network Intrusion Prevention System (IPS) High Availability (HA) feature enables appliances to work in an existing high availability network environment. The IPS passes all traffic over mirroring links, ensuring that both appliances see all traffic across the network and thus maintain state. This approach also allows the appliances to see asymmetrically routed traffic in order to fully protect the network.

HA support for Proventia Network IPS is limited to two cooperating appliances. Both appliances process packets inline, block attack traffic that arrives on their inline protection ports, and report events received on their inline ports to the management console.

For information on enabling HA, see "Enabling HA" on page 127.

Supported appliances

The following Proventia Network IPS appliance models can function in an existing HA environment:

- G400
- G2000
- GX5008
- GX5108
- GX6116

Use comparable models as a pair

Always use the same model appliances as an HA pair.

You cannot *mix* models in a single HA environment. For example, you cannot use a G2000 appliance and a GX5008 appliance as an HA pair.

Supported network configurations

High availability networks are typically configured in one of two ways:

Existing HA configuration	Description
Primary / Secondary	With this configuration, the traffic flows only on one of the redundant network segments and the primary devices on the network handle all of the traffic until one of the devices fails, at which point the traffic fails over to the secondary redundant network segment and the secondary devices take over.
Clustering	With this configuration, the traffic is load balanced and both sets of devices are active and see traffic all of the time.

Table 17: *Supported network configurations*

The Proventia HA feature supports both of these network configurations. In order to accomplish this, both Proventia appliances must maintain identical state. The appliances are connected by mirror links that consist of multiple connections over multiple ports. These mirror links pass all traffic an appliance receives on its inline ports to the other appliance, ensuring the protocol analysis modules on both appliances process all of the network traffic. In addition, the appliances also process asymmetrically routed traffic. This approach ensures that there is no gap in protection during failover.

Note: If you run Proventia Setup when the HA feature is enabled, you cannot modify network settings.

HA and SiteProtector management

You can manage HA through the SiteProtector Agent Manager. You must put both appliances in an HA configuration in the same SiteProtector group. SiteProtector can then synchronize appliance updates, including XPUs and policy updates. Each appliance reports to SiteProtector using a unique ID.

Processing responses

Both appliances process packets received from all redundant segments, but they only block attack traffic that arrives on their inline ports when appropriate. Both appliances report events to the management console at all times. However, they only process responses for events generated by packets that arrive on inline ports, and report those events to the Management Console. Appliances process but do not block or report events generated by traffic that arrives on mirroring ports.

As both appliances see all the traffic at all times, failover time for response processing is eliminated. Both appliances maintain current state, so if one HA network segment fails, the other appliance receives all packets on its inline ports, resulting in events being generated as soon as the network fails over.

Note: A small number of signatures, particularly for sweep attacks, such as Port Scans, can generate duplicate events, one by each appliance in a clustered configuration.

High availability modes

In an HA configuration, the appliance can operate in only inline simulation or inline protection mode. Passive monitoring mode is not supported. When you select an HA mode, all inline adapters are put in the corresponding adapter mode automatically.

HA does not address the availability or fault-tolerance of the appliances themselves. No separate high availability solution exists for appliances configured and wired for passive monitoring mode. You can configure appliances using the following high availability modes, as indicated in the following table:

Setting	Description
HA Simulation mode	Both HA partner appliances monitor traffic inline but do not block any traffic. Instead, both appliances monitor traffic and provide passive notification responses. The appliances also monitor traffic on each other's segment via mirror links – ready to take over notification in case of network failover.
HA Protection mode	Both HA partner appliances monitor traffic inline, and each report and block the attacks configured with block response, quarantine response, and firewall rules. The appliances also monitor traffic on each other's segment via mirror links – ready to take over reporting and protection in case of network failover.

Table 18: *HA appliance modes*

High Availability Configuration Overview

Introduction

Review the information in "High Availability Deployment" on page 37 before you configure the appliance.

For more information on configuring your firewall policy, see "Configuring Firewall Rules" on page 114.

Licensing

Licensing for an HA configuration is identical to licensing for a non-HA appliance; each individual appliance requests a single license from Site Protector (if you are using SiteProtector to manage the appliance).

Limitations

In HA mode, you cannot use adapter parameters as part of the firewall rules. You cannot define protection domains based on adapter. Because the same traffic may flow on different adapters in an HA environment, using adapter parameters may cause the two HA partner appliances to become unsynchronized.

Important: In protection domain definitions, the Adapter option must be set to 'Any'. In constructed firewall rule definitions, you must select all adapters. In manually created firewall rule definitions, the adapter keyword is invalid.

Proventia Manager

You can view HA configurations in Proventia Manager, as well as manage policies and updates, but ISS recommends you use SiteProtector to manage appliances in inline HA configurations.

Note: ISS recommends that you configure both HA partner appliances to use the same policies.

You can apply content updates and firmware updates serially so that one appliance is always operational in order to maintain network connectivity, particularly when both appliances are configured to fail closed.

High Availability Deployment

Introduction

This topic describes typical deployment scenarios for IPS in a high availability environment. It includes the following:

- a logical diagram for a standard HA deployment
- a physical network diagram for a standard deployment

Logical Diagram

You can manage the HA appliance cluster from Proventia Manager. If you use SiteProtector to manage the appliances, you can manage the HA cluster from the SiteProtector Agent Manager. A Logical HA diagram is shown in Figure 2:

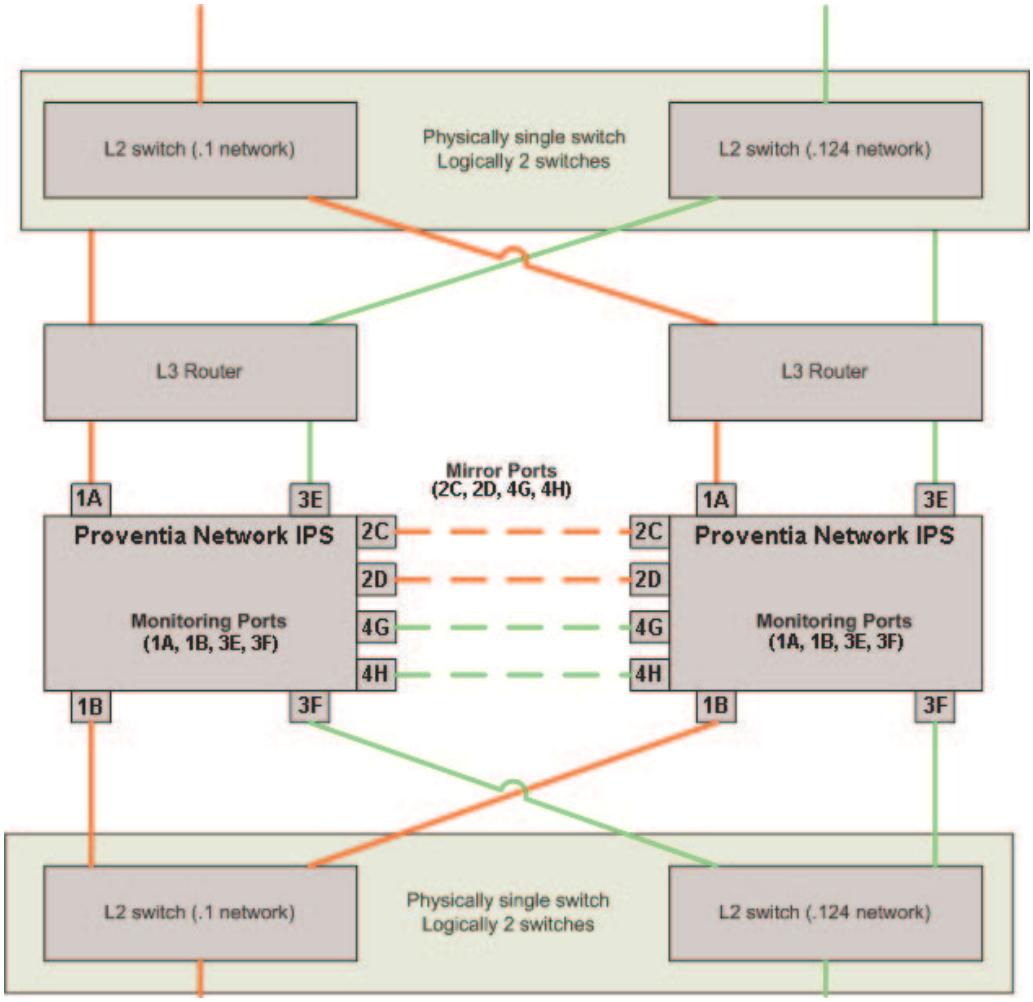

Figure 2: *Logical HA diagram for standard deployment*

Physical HA network diagram

A physical network diagram of a typical HA deployment scenario is shown in Figure 3:

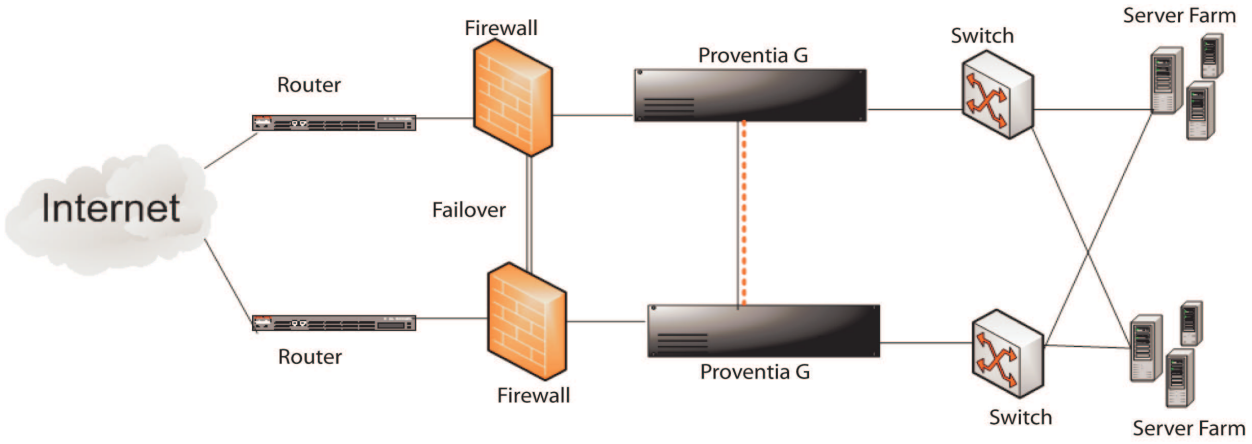

Figure 3: *HA physical network diagram*

Chapter 4

Using Proventia Manager

Overview

Introduction

This chapter describes how to use the local management interface to perform updates, make adjustments, and augment configuration settings.

In this chapter

This chapter contains the following topics:

Topic	Page
Completing the Configuration	40
Accessing Proventia Manager	42
Navigating Proventia Manager	43
Installing the License File	46
Working with Proventia Manager	47

Completing the Configuration

Introduction

After you have installed and configured the appliance, you can log in to Proventia Manager to complete the final configuration steps and set up appliance management.

Task overview

The following table outlines these steps:

Step	Description	Where to find the procedure
1	Contact your Sales Representative for the license registration number. Do the following: 1. Register your customer license at the ISS License Registration center (https://www1.iss.net/cgi-bin/lrc). 2. Download the license key file from the ISS Registration Center to your computer. **Note:** ISS recommends that you upload the license key file to a designated directory so that the appliance can download and install the latest updates automatically. You upload the license when you log in to Proventia Manager.	"Installing the license file" on page 46
2	Verify you have the following: • Internet Explorer version 6.0 or later • the recommended version of Java Runtime Environment (JRE), as noted in the Readme. The application prompts you with an installation link if you do not have it installed.	
3	Open Internet Explorer and log in to Proventia Manager as username **admin** and the password you configured during Proventia Setup.	"Logging on to Proventia Manager" on page 42
4	Install license.	"Installing the license file" on page 46
5	Apply updates.	"Updating the Appliance" on page 49

Table 19: *Setting up Proventia Manager*

Verifying setup

Verify that you have done the following:

1. Properly installed the hardware and connected the cables.
2. Created a connection using Hyperterminal (or a VT100 compatible terminal emulation program), with the recommended settings.
3. Completed all initial setup configurations, including the following:
   - logged on to the appliance with the Proventia Setup Utility
   - configured the admin, root, and Proventia Manager passwords
   - configured network settings
   - configured the time and date

- applied the settings

4. Prior to using the appliance, you must install the license file. Additionally, IBM ISS recommends that you complete the following tasks:
   - view your component status on the Home page
   - update the firmware
   - configure update settings
   - configure and update intrusion prevention settings
   - configure the firewall

Accessing Proventia Manager

Introduction

Proventia Manager is the Web-based management interface for the appliance.

Use Proventia Manager to perform the following tasks:

- monitor the status of the appliance
- configure and manage settings
- view quarantine table and apply changes
- review and manage appliance activities

Logging on to Proventia Manager

To log on to Proventia Manager:

1. Start Internet Explorer.
2. Type **`https://xxx.xxx.xxx.xxx`**
   where **`xxx.xxx.xxx.xxx`** is the appliance's IP address.
3. Log in using the user name **`admin`** and the Proventia Manager password.
4. If a message informs you that you do not have Java Runtime Environment (JRE) installed, install it, and then return to this procedure.
5. Select **Yes** to use the Getting Started procedures.

   Note: ISS recommends that you use the Getting Started procedures to help you customize the appliance settings. If this window does not appear, you can also access the Getting Started procedures from the Help.
6. Click **Launch Proventia Manager**.

Navigating Proventia Manager

Introduction

If you are planning to use Proventia Manager to manage the appliance, you should familiarize yourself with its navigation features.

About the navigation buttons

The following buttons appear on every page in Proventia Manager:

Click this button...	To do this...
SYSTEM LOGS	Access the System Logs page.
ALERTS	Access the Alerts page for the area you have selected in the left navigation pane.
HELP	Access the online Help.
	Minimize or maximize the navigation pane.

Table 20: *Navigation buttons*

About the left navigation pane

In the left pane, you select the item in the tree that you want to configure. Some items have more than one component for you to configure. Expand the tree to display a list of configurable elements in that area.

The following table describes each area of Proventia Manager:

This item...	Lets you view or configure...
Notifications	In the Notifications area, you can view high-level Alert Event Log information, System Logs, system (appliance) alert information. See “Viewing Alerts and System Information” on page 141 for more information.
Intrusion Prevention	In the Intrusion Prevention area, you can configure responses, protection domains, and event types that help keep the network secure from intrusions. You can also view important security alert and quarantined intrusion information, and determine how the appliance should respond to detected intrusions. See the following topics for more information: • “Working with Security Events” on page 77 • “Configuring Responses” on page 67 • “Configuring Other Intrusion Prevention Settings” on page 91
Firewall Settings	In the Firewall Settings area, you can create and edit firewall rules to block attacks. See “Configuring Firewall Settings” on page 113 for more information.

Table 21: *Left navigation pane*

This item...	Lets you view or configure...
System	In the System area, you can configure and view information about the appliance. You can configure user access, network adapter cards, alerts, and advanced parameters to help you monitor the appliance. You can also view and download important system logs, manage licenses, and reboot the appliance from this area. See the following topics for more information: • "Configuring Local Tuning Parameters" on page 121 • "Managing System Settings" on page 135
Statistics	The Statistics area lets you view important statistics about appliance activity, such as Protection, Packet, and Network information. See "Viewing Statistics" on page 147 for more information.
Updates	Use the Updates area to configure and manage updates for the appliance, so that you have the latest protection available for your network. See "Updating the Appliance" on page 49 for more information.
Support	The Support area provides contact information for Technical Support, as well as helpful links to provide you assistance with the appliance. See "Getting Technical Support" on page 10 for more information.

Table 21: *Left navigation pane (Continued)*

About icons

The following table describes icons that appear in Proventia Manager as you work:

Icon	Description
	Click this icon to add an item to the list.
	Click this icon to edit an item in the list.
	Click this icon to remove an item (or items) from the list. You can use the standard SHIFT+click or CTRL+click methods to select adjacent or non-adjacent items in the list. **Note**: In some cases, when you click Remove, an item is not removed from the list, but it is disabled and reset to its default state.
	Click this icon to group items by column in a table. For example, you could group security events by severity. This means that your high, medium, and low severity events each have their own group, making it easier for you to search for events.
	Click this icon to reset table groupings to their default settings.
	Click this icon to select the columns you want to display on a page.
	Select an item in the list and click this icon to move the item up the list.
	Select an item in the list and click this icon to move the item down the list.
	Select an item in the list and click this icon to copy the item to the clipboard. **Tip**: You can use the standard SHIFT+click or CTRL+click methods to select adjacent or non-adjacent items in the list.

Table 22: *Proventia Manager policy icons*

Icon	Description
	Click this icon to paste a copied item from the clipboard into a list. After you paste the item, you can edit it.
	If this icon appears on a page or next to a field on a page, then you must enter required data in a field, or the data you have entered in a field is invalid.

Table 22: *Proventia Manager policy icons (Continued)*

About saving changes

Each time you navigate from one location to another in Proventia Manager, click **Save Changes** to ensure that the changes are applied. If you do not save information before navigating to another page, you are prompted to save your information. To move to another page without saving changes, click **Cancel Changes** so that you are not prompted to save before you click the new link.

Installing the License File

Introduction

Proventia Network IPS appliances require a properly configured license file. If you have not installed the appropriate license file, you cannot manage the appliance.

Each individual appliance requests a single license from SiteProtector. Licensing for an appliance in a high-availability configuration is identical to licensing for any other appliance.

To purchase a license, contact your local sales representative.

Use the procedure below to install the license file. This is necessary to make your appliance run at full capability. Installation involves saving the license file information to the appropriate location so that Proventia Manager can locate and acknowledge it.

Prerequisites

Before you install the license file, complete the following:

- register your customer license
- download the license from the ISS Registration Center

About the Licensing page

The Licensing page displays important information about the current status of the license file, including expiration dates. Additionally, this page allows you to access the License Information page, which includes information about how to acquire a current license.

Installing the license file

To install the license file:

1. In Proventia Manager, select **System→Licensing**.
2. Click **Browse**.
3. Locate the license file that you downloaded.
4. Click **OK**.
5. Click **Upload**.

Working with Proventia Manager

Introduction

When you open Proventia Manager, the Home page provides an immediate snapshot of the current status of the appliance. This page includes the following navigation, information and reporting options:

- device name (the appliance domain name you configured during setup)
- protection status
- system status
- alerts for each module
- important messages

Viewing protection status

The protection status area describes the current status of the intrusion prevention component. Selecting a component name links you to the component status page.

The following status icons show you the current status of a component:

Icon	Description
	Indicates that the component is active.
	Indicates that the component is stopped.
	Indicates that the component is in an unknown state. This status may require immediate attention.

Table 23: *Protection status icons*

Viewing system status

On the Home page, the system status group box describes the current status of the system.

The following table describes the data available in the System Status area:

Statistic	Description
Model Number	The model number of the appliance.
Base Version Number	The base version of the appliance software. **Note:** The base version is the software version shipped with the appliance, or the software version of the most recent firmware update.
Uptime	How long the appliance has been online, in the following format: `x days, x hours, x minutes`
Last Restart	The last time the appliance was restarted, in the following format: `yyyy-mm-dd hh:mm:ss` **Example:** `2004-05-04 16:24:37`
Last Firmware Update	The last time appliance firmware was updated, in the following format: `yyyy-mm-dd hh:mm:ss - version: x.x` **Example:** `2004-05-04 16:25:56 - version: 1.7`

Table 24: *System Status statistics*

Statistic	Description
Last Intrusion Prevention Update	The last time appliance security content was updated, in the following format: `yyyy-mm-dd hh:mm:ss - version: x.x` **Example:** `2004-01-25 12:34:36 - version: 1.7`
Last System Backup	The last time a system backup was created, in the following format: `yyyy-mm-dd hh:mm:ss` **Example:** `2004-05-04 15:49:01`
Backup Description	The backup type on the appliance: • Factory Default • Full System Backup

Table 24: *System Status statistics (Continued)*

Viewing important messages

The Home page displays important messages about licensing and updates. If you have not configured the appliance to download updates automatically, these messages may appear with a link to the appropriate Proventia Manager page.

Chapter 5

Updating the Appliance

Overview

Introduction

This chapter describes how to update the appliance using Proventia Manager. You can manually download and install firmware updates and security updates, or you can configure the appliance to automatically download and install some or all updates at designated times.

In this chapter

This chapter contains the following topics:

Topic	Page
Updating the Appliance	50
Updating the Appliance Automatically	52
Updating the Appliance Manually	54
Using Update Tools	55
Using Advanced Parameters to Tune Update Settings	56

Updating the Appliance

Introduction

Ensure the appliance is always running the latest firmware and intrusion prevention updates. The appliance retrieves updates from the ISS Download Center, accessible over the Internet.

You can update the appliance in two ways:

- configure automatic updates
- find, download, and install updates manually

Types of updates

You can install the following updates:

- **Firmware updates**. These updates include new program files, fixes or patches, enhancements, or online Help updates.
- **Intrusion prevention updates**. These updates contain the most recent security content provided by ISS's X-Force.

You can find updates on the Updates to Download page, and you can schedule automatic update downloads and installations from the Update Settings page.

Note: Some firmware updates require you to reboot the appliance. For more information about product issues and updates, see the Proventia Network Intrusion Prevention System (IPS) Readme on the ISS Download Center at http://www.iss.net/download/.

Finding available updates

When you click **Find Updates** on the Update Status page, the appliance checks for the following:

- updates already downloaded to the appliance and ready to be installed
- updates available for download from the ISS Download Center

If the appliance finds updates to download or install, an alert message displays a link to the appropriate page (the Download Updates or Install Updates page).

Update packages and rollbacks

A rollback removes the last intrusion prevention update installed on the appliance. You cannot roll back firmware updates.

Important: IBM ISS recommends that you perform a full system backup before you install a firmware update. If you enable automatic firmware updates, you should enable the Perform Full System Backup Before Installation option.

After an update is installed, the appliance deletes the update package so the downloaded package is no longer on the appliance. If you roll back the update, the appliance is available for update downloads and installation the next time updates are available or at the next scheduled automatic update.

SiteProtector management

If you use SiteProtector to manage the appliance, you can install an update while the appliance is registered with the SiteProtector Agent Manager. You can also configure it to use the SiteProtector X-Press Update Server to download and install available updates.

Consider using the X-Press Update Server under the following conditions:

- **Large number of appliances.** If you have deployed a large number of appliances, you can save bandwidth. The appliances can request updates from one Update Server, as opposed to using bandwidth to download the same updates for each appliance from the ISS Download Center.
- **Locked down environment.** If you want to download updates in a more secure environment and do not want every appliance to have Internet access for downloads, the appliance can request updates from the Update Server. In this case, only the Update Server requires the Internet connection.

See the SiteProtector documentation or online help for information about configuring the X-Press Update Server.

Virtual Patch technology

Automatic security updates come from ISS X-Force using Virtual Patch technology. The Virtual Patch process protects systems against attack during the interval between discovery of a vulnerability and the manual application of a security patch.

The Virtual Patch is an important component of ISS's Dynamic Threat Protection platform. By combining the functionality of vulnerability detection, intrusion protection, management, and advanced correlation tools, you can have a unified view of system-wide intrusion protection capabilities to protect against known and unknown threats.

Troubleshooting download problems

If you experience problems in Proventia Manager after you apply a firmware update, try the following steps:

1. Close the Web browser.
2. Clear the Java cache.
3. Restart the Web browser.
4. Log on to Proventia Manager.

For more information about how to clear the Java cache, refer to the operating system documentation.

Updating the Appliance Automatically

Introduction

Use the Update Settings page to configure the appliance to automatically check for and install updates. Define the following settings to configure automatic updates for the appliance:

- when to check for updates
- when to download and install security updates
- when to download firmware updates
- how and when to install firmware updates
- which firmware update version(s) to install

Note: When you install a firmware update, the appliance may lose link temporarily.

Example

Let's say you want to configure the appliance to check for updates daily at 3:00 A.M. If it finds any updates (either firmware or security updates), you want it to automatically download all of the updates, and then install the security updates immediately. As the final steps, at 5:00 A.M., you want the appliance to automatically perform a system backup and then install the available firmware updates.

The following table describes the appliance update process with these settings:

Stage	Description
1	At 3:00 AM, the appliance checks the ISS Download Center for updates.
2	The appliance downloads security and firmware updates.
3	The appliance installs security updates immediately.
4	At 5:05 AM, the appliance does the following: • reboots, and then creates a system backup • installs the firmware update, and then reboots if necessary

Table 25: *An example of the update process*

Procedure

To update the appliance automatically:

1. On the **Update Settings** page, complete or change the settings as indicated in the following table.

Section	Setting	Description
Automatically Check for Updates	Check for updates daily or weekly	If you enable this option, select the **Day Of Week** and **Time Of Day** the appliance should check for updates. **Note**: Set the appliance to check for updates at least one (1) hour prior to installing scheduled automatic updates to ensure the appliance has downloaded all the necessary updates.
	Check for updates at given intervals	Checks for updates several times a day. Type a value in the **Interval (minutes)** box, or move the slider bar to select a value. The minimum interval is 60 minutes; the maximum is 1440.
Security Updates	Automatically Download	Automatically downloads security updates.
	Automatically Install	Automatically installs security updates.
Firmware Updates	Automatically Download	Automatically downloads firmware updates.
Firmware Updates - Install Options	Perform Full System Backup Before Installation	Enables the appliance to reboot and perform a full system backup before it installs any updates. **Note**: Each time the appliance performs a backup, it overwrites the previous system backup.
	Do Not Install	Downloads firmware updates but does not install them. See "Updating the Appliance Manually" on page 54 for more information.
	Automatically Install Updates	Automatically installs firmware updates. **Note**: When the appliance automatically installs updates, it may be offline for several minutes.
Firmware Updates - When To Install	Delayed	Installs updates on the **Day Of Week** and **Time Of Day** you specify. **Note**: You must configure automatic installation to occur at least one (1) minute after the appliance has completed downloading updates.
	Immediately	Installs updates as soon as they are downloaded. **Important**: ISS does not recommend this option.
	Schedule One Time Install	Installs one update instance at the **Date** and **Time** you specify.
Firmware Updates - Which Version To Install	All Available Updates	Installs all update versions, including the most recent one.
	Up To Specific Version	Installs all versions up to the **Version** number you specify.

2. Save your changes.

Updating the Appliance Manually

Introduction

You can update the appliance manually in either of the following circumstances:

- you have not configured automatic updates for the appliance
- you want to install an available update off-schedule

Process overview

You must complete the following tasks to update the appliance manually:

- locate and download available updates
- install the updates

Note: When you install a firmware update, the appliance may lose link temporarily.

Finding and downloading available updates

To find and download available updates:

1. In Proventia Manager, select **Updates→Available Downloads**.
2. If your appliance model requires it, the Export Administration window appears.

   Review the agreement, select **Yes**, and then click **Submit**.
3. The Updates to Download window appears and displays the following message if updates are available: "There are updates available. Click here to see details."

   Click the link in the message.
4. On the Updates to Download page, click **Download All Available Updates**.

Installing updates

To install updates:

1. In Proventia Manager, select **Updates→Available Installs**.
2. If your appliance model requires it, the Export Administration Regulation window appears.

   Review the agreement, select **Yes**, and then click **Submit**.
3. On the Available Installs page, select the updates you want to install, and then click **Install Updates**.

   Note: Some firmware updates require you to reboot the appliance. For detailed information about each firmware update, review the Proventia Network Intrusion Prevention System Readme on the ISS Download Center at http://www.iss.net/download/.
4. View the installation status in the Update History table on the Update Status page.

Using Update Tools

Introduction

Use the Update Tools page to find updates or to roll back an update. A rollback removes the last update installed on the appliance.

Important: You cannot roll back firmware updates.

Cumulative updates and rollbacks

XPU updates are cumulative.

Example

The following example describes how the appliance behaves when rolling back cumulative updates:

If you install security update 1.81 but do not install version 1.82, and then you install version 1.83, version 1.82 is installed with version 1.83.

However, if you roll back from version 1.83, the appliance does not roll back to version 1.82. A rollback to the last applied update takes the appliance back to version 1.81.

Update packages and rollbacks

After an update is installed, the appliance deletes the update package, so the downloaded package is no longer on the appliance. If you roll back the update, then that update appears as available for download and installation the next time you find updates or at the next scheduled automatic update. For more information, see "Updating the Appliance Automatically" on page 52.

Finding available updates

To find available updates:

1. In Proventia Manager, select **Updates→Tools**.
2. Click **Find Updates**.
3. If the appliance finds updates to download or install, an alert message displays the link to the Available Downloads or Available Installs page.

   Click the appropriate link to download or install the latest updates.

Rolling back updates

To roll back updates:

1. In Proventia Manager, select **Updates→Tools**.
2. Click **Rollback Last Intrusion Prevention Update**, and then click **OK**.
3. Press F5 to refresh the page and check the progress of the rollback.

Using Advanced Parameters to Tune Update Settings

Introduction

Use the Advanced Parameters tab on the Update Settings page to tune the update settings.

About advanced parameters

Advanced parameters are composed of name/value pairs. Each name/value pair has a default value.

For example, the parameter np.firewall.log is a parameter that determines whether to log the details of packets that match firewall rules you have enabled. The default value for this parameter is *on*.

You can edit the value of any parameter that appears in the list on the Advanced Parameters tab. If the parameter does not appear in the list, it does not mean the parameter has no default value. You simply need to add the parameter to the list with the new value.

Advanced parameters for updates

The appliance contains the following pre-configured update advanced parameters, listed in Table 26:

Note: Only the first two parameters appear on the Update Settings Advanced Parameters tab if you are managing the appliance through Proventia Manager. If you have enabled SiteProtector management, you can configure the other default parameters for communicating with SiteProtector's Update Server.

Parameter	Type	Default Value	Description
Update.disable.remote.discovery	boolean	false	Specifies whether the appliance should look for updates on the Internet.
Update.preserve.update.files	boolean	false	Specifies whether to delete update files once they have been successfully installed.
Update.certificate.file	string	etc/httpd/conf/ss.crt/ca-bundle.crt	Specifies the SSL Cert Authority file to use when connecting to the Update Server.
Update.proxy.auth	boolean	false	Authorizes the use of the HTTP proxy server when connecting to the Update Server.
Update.proxy.enable	boolean	false	Enables the use of the HTTP proxy server when connecting to the Update Server.
Update.proxy.password	string	none	Specifies the password to the HTTP proxy server authentication for connecting to the Update Server.

Table 26: *Update advanced parameters*

Parameter	Type	Default Value	Description
Update.proxy.port	number	none	Specifies the port number of the HTTP proxy server for connecting to the Update Server.
Update.source.url	string	https://www.iss.net/XPU If the appliance is not connected to the Internet, use https//:<Update Server IP Address or name>:3994/xpu (Name is case sensitive.)	Specifies the address of the Update Server.
Update.proxy.user	string	none	Specifies the user name to the HTTP proxy server authentication for connecting to the Update Server.

Table 26: *Update advanced parameters*

Adding advanced parameters

To add advanced parameters:

1. Select **Update Settings**.
2. If needed, review the Export Agreement, select **Yes**, and then click **Submit**.
3. Select the **Advanced Parameters** tab.
4. Click **Add**.
5. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a unique name for the parameter.
Comment	Type a unique description for the parameter.
Value	Select one of the following values: • **Boolean**. Select the Enabled check box to set the value as True, or clear it to set the value as False. • **Number**. If you select this option, type a numeric Value. • **String**. If you select this option, type the associated text string Value.

6. Click **OK**.
7. Save your changes.

Working with advanced parameters

To edit, copy, or remove update advanced parameters:

1. Select **Update Settings**.
2. Select the **Advanced Parameters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Advanced Parameters tab by double-clicking the item you want to configure. 1. Select the parameter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the parameter, and then click **OK**.
Copy	1. Select the parameter, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the parameter as needed, and then click **OK**.
Remove	1. Select the parameter. 2. Click the **Remove** icon.

3. Save your changes.

Chapter 6

Managing the Appliance through SiteProtector

Overview

Introduction

This chapter describes how to set up the appliance so you can manage it through the SiteProtector Console.

In this chapter

This chapter contains the following topics:

Topic	Page
Managing with SiteProtector	60
Configuring SiteProtector Management	62
Navigating SiteProtector	65

Managing with SiteProtector

Introduction

SiteProtector is the IBM ISS management console. With SiteProtector, you can manage components and appliances, monitor events, and schedule reports. By default, your appliance is set up for you to manage it through Proventia Manager. If you are managing a group of appliances along with other sensors, you may prefer the centralized management capabilities that SiteProtector provides.

What you manage with SiteProtector

When you register the appliance with SiteProtector, SiteProtector controls the following management functions of the appliance:

- Firewall settings
- Intrusion prevention settings
- Alert events

To change any settings for the functions listed here, you must use SiteProtector.

You can manage update and installation settings in Proventia Manager or in SiteProtector.

Note: When you register the appliance with SiteProtector, some areas of Proventia Manager become read-only. When you unregister the appliance from SiteProtector, Proventia Manager becomes fully functional again.

What you manage with Proventia Manager

You must manage the following local functions directly on the appliance, even when the appliance is registered with SiteProtector:

- enabling or disabling SiteProtector management
- viewing quarantined intrusions
- deleting quarantine rules
- manual updates

How the SiteProtector Agent Manager works

When you enable SiteProtector management, you assign the appliance to an Agent Manager. Agent Managers manage the command and control activities of various agents and appliances registered with SiteProtector and facilitate data transfer from appliances to the Event Collector, which manages real-time events it receives from appliances.

The Agent Manager sends any policy updates to appliances based on their policy subscription groups. (A subscription group is a groups of agents or appliances that share a single policy.) Decide which group the appliance should belong before you register it with SiteProtector. Eventually, the group's policy is shared down to the appliance itself.

For more information about the Agent Manager, see the SiteProtector documentation or online Help.

How SiteProtector management works

When you register the appliance with SiteProtector, the appliance sends its first *heartbeat* to the Agent Manager to let the Agent Manager know that it exists. A heartbeat is an encrypted, periodic HTTP request the appliance uses to indicate it is still running and to allow it to receive updates from the Agent Manager. When you register the appliance with SiteProtector, you set the time interval (in seconds) between heartbeats.

When the Agent Manager receives the heartbeat, it places the appliance in the group you specified when you set up registration. If you did not specify a group, it places the appliance in the default group "G-Series" or "Network IPS," depending on your version of SiteProtector. If you clear the group box when you register the appliance, it places the appliance in Ungrouped Assets.

Local settings or policy settings

If you opted to allow local appliance settings to override group settings, then the appliance maintains its local settings at the first heartbeat. If you did not allow local appliance settings to override group settings, then the Agent Manager immediately "pushes" the group's policy files to the appliance, even if the group's policy settings are undefined. For example, if you set firewall rules on the appliance and then you register the appliance with a group that has no firewall rules defined, the group policy overwrites the local policy, and the appliance no longer has firewall rules enabled.

At the second heartbeat and each heartbeat thereafter, the Agent Manager "pushes" the group policy to the appliance. However, you can change some local appliance settings through SiteProtector. Any local policy settings you change for the appliance take precedence over the group policy settings for that appliance only; the group policy settings remain in effect for all other appliances in the group.

How appliance updates work with SiteProtector

After you register the appliance with SiteProtector, you must continue to update it regularly to maximize performance and to ensure it runs the most up-to-date firmware, security content, and database. Consider scheduling automatic database updates, security content updates, and firmware update downloads and installations.

Note: You can download and install firmware updates in Proventia Manager even if the appliance is registered with SiteProtector.

Use the Update Settings page to schedule the following automatic update options:

- downloading and installing firmware updates
- downloading and installing security content updates
- updating the database

How appliance events are handled in SiteProtector

You can specify the events that generate and deliver an alert to SiteProtector. When an event occurs, the appliance sends an alert to SiteProtector. You can use the event information in the alert to create valuable reports. The alerts sent to SiteProtector still appear in the Alerts page in Proventia Manager if the alerts are configured for logging.

SiteProtector management options

When you register the appliance with a SiteProtector group, you can do the following:

- Allow the appliance to inherit sensor group settings
- Manage some or all of settings for a single appliance in the group independently in SiteProtector, so that the appliance maintains those individual settings regardless of group settings

Configuring SiteProtector Management

Introduction

Enabling SiteProtector management automatically does the following:

- Registers the appliance with SiteProtector
- Places the appliance in a specified SiteProtector group
- Directs the appliance to report to a specified Agent Manager

Use the Management page in Proventia Manager to set up and enable SiteProtector management for the appliance.

After you have registered your appliance, you must add the Proventia Network IPS license file in SiteProtector. This enables you to apply updates through SiteProtector. See your SiteProtector documentation for more information about adding license files for agents and appliances.

Important: To manage the appliance with SiteProtector, you must run SiteProtector version 2.0 Service Pack 6 or later.

Before registering the appliance

Do the following before you register the appliance with SiteProtector:

- Verify the name of the SiteProtector sensor group to which you want to assign the appliance.
- Verify the IP address and port for each SiteProtector Agent Manager that you want to use with the appliance.
- Ensure that the appliance has the latest firmware update installed.

You can schedule automatic downloads and installations of firmware updates to the appliance without unregistering the appliance from SiteProtector.

Reference: See "Updating the Appliance" on page 49 for more information.

Configuring SiteProtector management

To configure SiteProtector management:

1. In Proventia Manager, select **System→Management**.
2. Complete or change the settings as indicated in the following table.

Setting	Description
Register with SiteProtector	Select the check box to register the appliance with SiteProtector.
Local Settings Override SiteProtector Group Settings	Select this option to have the appliance maintain any local settings you have configured *at the first heartbeat*. If you do not select this option, the appliance inherits the settings of the SiteProtector group you specify *at the first heartbeat*. **Note**: At the second heartbeat and each heartbeat thereafter, any policy settings you have changed at the group level are sent to the appliance.

Setting	Description
Desired SiteProtector Group for Sensor	Type the name of the SiteProtector group to which the appliance should be assigned. If you do not specify a group, then the appliance is added to the default “G-Series” or “Network IPS” group. **Important**: You must assign the appliance to a group that contains only other Proventia Network IPS or G-Series appliances.
Heartbeat Interval (secs)	Type the number of seconds the appliance should wait between sending heartbeats to SiteProtector. **Note**: This value must be between 300 and 86,400 seconds.

3. Click **Save Changes**.
4. Add the Agent Manager(s) with which you want the appliance to communicate. See "Configuring the Agent Manager.”

Configuring the Agent Manager

To configure the Agent Manager:

1. In Proventia Manager, select **System→Management**.
2. Ensure you have enabled registration with SiteProtector.
3. In the Agent Manager Configuration area, click **Add**.
4. Complete or change the settings as indicated in the following table.

Setting	Description
Authentication Level	Select an option from the list. **Note**: We recommend that you accept the default option *first-time trust*.
Agent Manager Name	Type the Agent Manager name exactly as it appears in SiteProtector. This setting is case-sensitive.
Agent Manager Address	Type the Agent Manager's IP address.
Agent Manager Port	Accept the default value 3995. **Note**: You can type a new port number, but you must also configure the new port number locally on the Agent Manager itself.
User Name	If the appliance must log into an account to access the Agent Manager, type the user name for that account here. **Note**: The account user name is set on the Agent Manager.
User Password	Click **Set Password**, type and confirm the password, and then click **OK**.
Use Proxy Settings	If the appliance must go through a proxy to access the Agent Manager, select the **Use Proxy Settings** check box, and then type the **Proxy Server Address** and **Proxy Server Port**.

5. Click **OK**.
6. Click **Save Changes**.

Verifying successful registration

To verify that the appliance registered successfully with SiteProtector:

1. Open the SiteProtector Console.
2. In the left pane, select the group to which you added the appliance.

   Note: If you did not specify a group when you registered appliance, it appears in the default group "G-Series" or "Network IPS," depending on your version of SiteProtector. If you cleared the default group, the appliance may appear in Ungrouped Assets.
3. Select the **Sensor** or **Agent** tab.

   The appliance appears on the Sensor tab, and its status appears as "Active."

Disabling SiteProtector Management

To disable SiteProtector management:

1. In Proventia Manager, select **System→Management**.
2. Clear the **Register with SiteProtector** check box.
3. Click **Save Changes**.

Navigating SiteProtector

Introduction

If you are planning to use SiteProtector to manage the appliance, you should familiarize yourself with the navigation features that allow you to create, manage, and view the appliance's current IPS policies.

For general information about navigating the SiteProtector Console, see the SiteProtector Help.

About policies and settings

You can configure the following appliance policies and settings in SiteProtector:

Select this item...	To do this...
Intrusion Prevention	Configure responses, protection domains, and event types that help keep the network secure from intrusions. You can also view important security alert and quarantined intrusion information, and determine how the appliance should respond to detected intrusions. See the following topics for more information: • "Working with Security Events" on page 77 • "Configuring Responses" on page 67 • "Configuring Other Intrusion Prevention Settings" on page 91
Firewall Settings	Create and edit firewall rules to block attacks. See "Configuring Firewall Settings" on page 113 for more information.
Local Tuning Parameters	Configure local tuning parameters for the appliance, including: • appliance error, warning, and informational alerts • network adapter card settings • advanced parameters for the appliance itself, including update parameters, firewall parameters, and intrusion prevention parameters See "Configuring Local Tuning Parameters" on page 121 for more information.
Statistics	View important statistics about appliance activity, such as Protection, Packet, and Network information. See "Viewing Statistics" on page 147 for more information.
Updates	Configure and manage updates for a single appliance, so that you have the latest protection available for the network. See "Updating the Appliance" on page 49 for more information.

Table 27: *Policies and settings*

About icons

The following table describes icons that appear on the Policy page as you work:

Icon	Description
	Click this icon to add an item to the list.
	Click this icon to edit an item in the list.

Table 28: *Policy editor icons in SiteProtector*

Icon	Description
	Click this icon to remove an item (or items) from the list. You can use the standard SHIFT+click or CTRL+click methods to select adjacent or non-adjacent items in the list. **Note**: When you click Remove, an item may not be removed from the list; instead, it is disabled and reset to its default state.
	Click this icon to group items by column in a table. For example, you could group security events by severity. The high, medium, and low severity events will each have their own group, making it easier for you to search for events.
	Click this icon to reset table groupings to their default settings.
	Click this icon to select the columns you want to display on a page.
	Select an item in the list and click this icon to move the item up the list.
	Select an item in the list and click this icon to move the item down the list.
	Select an item in the list and click this icon to copy the item to the clipboard. **Tip**: You can use the standard SHIFT+click or CTRL+click methods to select adjacent or non-adjacent items in the list.
	Click this icon to paste a copied item from the clipboard into a list. After you paste the item, you can edit it.
	This icon indicates that information is missing or invalid. If this icon appears on a page or next to a field on a page, then you need to enter or correct the required data in a field.

Table 28: *Policy editor icons in SiteProtector*

Opening an IPS policy in SiteProtector

To open an IPS policy in SiteProtector:

1. In the SiteProtector Console, do one of the following
   - To edit a group level policy, right-click the group in the left pane, and then select **Manage Policy** on the pop-up menu.
   - To edit a policy for a single appliance, on the **Agent** tab, right-click the appliance, and then select **Manage Policy** on the pop-up menu.
2. On the Policy tab, select Network IPS from the **Agent Type** drop-down menu.
3. To open the policy, do one of the following:
   - Select the policy for the group or appliance in the left pane. The policy opens in the right pane.
   - Select the group or appliance in the left pane, and then right-click the policy in the right pane and select **Manage Policy** on the pop-up menu.

   Note: To ensure that a policy at the group or appliance level overrides a policy at the Site level, right-click the policy, and then select Override. See "Configuring Policy Inheritance" in the SiteProtector Help for more information.
4. Edit the policy as necessary.
5. Click **Save All** on the toolbar to save your changes.

Chapter 7

Configuring Responses

Overview

Introduction

This chapter describes how to configure responses for the appliance. Responses control how the appliance reacts when it detects an intrusion or other important events on the network.

In this chapter

This chapter contains the following topics:

Topic	Page
About Responses	68
Configuring Email Responses	69
Configuring the Log Evidence Response	71
Configuring Quarantine Responses	72
Configuring SNMP Responses	73
Configuring User Specified Responses	75

About Responses

Introduction

Your response policy controls how the appliance responds when it detects intrusions or other important events. You create responses and then apply them to events as necessary.

You can configure the following response types:

- **Email**. Send email alerts to an individual address or email group.
- **Log Evidence**. Log alert information to a saved file.
- **Quarantine**. Quarantine the attack.
- **SNMP**. Send SNMP traps to a consolidated SNMP server.
- **User Specified**. Process alerts using your custom programs or scripts.

Block response

The Block response is a default response that blocks attacks by dropping packets and sending resets to TCP connections. The Block response differs depending on the appliance's operation mode, as follows:

In this mode...	The appliance...
Passive Monitoring	Responds to intrusions with a traditional block response.
Inline Simulation	Monitors network traffic and generates alerts but does not block the offending traffic.
Inline Protection	Blocks attacks by dropping packets and sending resets to TCP connections.

Table 29: *Appliance modes and the Block response*

The appliance mode is set when the appliance is installed. For more information, see "Managing Network Adapter Cards" on page 125.

Ignore response

You can set the Ignore response for security events, which tells the appliance to disregard packets that match criteria specified within an event. You can also set this response through response filters. If you select this response when you create response filters or security events, the appliance does not act when it detects the matching packets.

Use the Ignore response only to filter security events that do not threaten the network. For more information, see "Configuring Response Filters" on page 86.

Response objects in SiteProtector

If you are managing the appliance through SiteProtector and you want to configure responses for events, select Response Objects. Response objects enable you to centralize data. If the data changes, you can modify the response object instead of each instance of the data.

Note: If you are using SiteProtector to manage the appliance, ISS recommends that you use Central Responses to create event responses. See "Configuring Central Responses" in the SiteProtector Help for more information.

Configuring Email Responses

Introduction

You can configure email notifications to alert individuals or groups when specific events occur. You can also select the event parameters to include in the message to provide important information about detected events.

Adding email responses

To add or change email responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **Email** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a meaningful name for the response. **Tip**: This name appears when you select responses for events, so you should give the response a name that allows users to easily identify what they are selecting.
SMTP Host	Type the fully qualified domain name or IP address of the mail server. **Note**: The SMTP Host must be accessible to the appliance to send email notifications.
From	Type an email address. Separate email addresses with semicolons.
To	Type an email address. Separate email addresses with semicolons.
Sensor Parameters	Type a **Subject** and **Body** for the message. You can also expand the list and select parameters to add to the message. The appliance populates valid parameters for the event; any invalid parameters retain the original tag format, such as <ObjectName>.

5. Click **OK**.
6. Save your changes.

Working with email responses

To edit, copy, or remove email responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **Email** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Email tab by double-clicking the item you want to configure. 1. Select the response, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the response, and then click **OK**.
Copy	1. Select the response, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the response as needed, and then click **OK**.
Remove	1. Select the response. 2. Click the **Remove** icon.

3. Save your changes.

Configuring the Log Evidence Response

Introduction

You can configure the appliance to log the summary of an event. The Log Evidence response creates a copy of the packet that triggers an event and also records information that identifies the packet, such as Event Name, Event Date and Time, and Event ID. Evidence logs show you what an intruder did or tried to do to the network.

The appliance logs packets that trigger events to the `/var/iss/` directory.

Configuring the log evidence response

To configure the log evidence response:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **Log Evidence** tab.
3. Complete or change settings as indicated in the following table:

Setting	Description
Maximum Files	Type the maximum number of files that the log can store. The default is 10 files. When the log reaches the maximum file number, it begins again with zero (0) and overwrites the existing files.
Maximum File Size (in KB)	Type the maximum file size the log can store. The default is 10000 KB.
Log File Prefix	Type the log file name prefix. The default is "evidence."
Log File Suffix	Type the log filename extension. The default is ".enc"

4. Save your changes.

Configuring Quarantine Responses

Introduction

You can create quarantine responses that block intruders when the appliance detects security, connection, or user-defined events. These responses also block worms and trojans. Quarantine responses work only when you have configured the appliance to run in Inline Protection mode.

Note: The Quarantined Intrusions page shows rules dynamically generated in response to detected intruder events. For more information, see "Managing Quarantined Intrusions" on page 92.

Pre-defined quarantine responses

The following table describes the three pre-defined responses that exist for the appliance:

Quarantine objects	Description
Quarantine Intruder	Fully blocks both machines involved in an attack.
Quarantine Trojan	Isolates any machine that is the victim of an attack.
Quarantine Worm	Isolates the item the worm is trying to find; for example, a SQL port.

Table 30: *Pre-defined response objects*

Note: You can change the settings for these pre-defined responses, but you cannot rename or remove them.

Adding or changing quarantine responses

To add or change quarantine responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **Quarantine** tab.
3. Click **Add**, or highlight the response you want to edit, and then click **Edit**.
4. Complete or change the settings as indicated in the following table.

Setting	Description
Name	Type a meaningful name for the response. **Tip**: This name appears when you select event responses, so give the response a name that users can easily identify.
Victim Address	Block packets based on target IP address.
Victim Port	Block packets based on target port.
Intruder Address	Block packets based on source IP address.
Intruder Port	Block packets based on source port.
ICMP Code	Block packets based on the ICMP code number (if protocol is 1).
ICMP Type	Block packets based on the ICMP type number (if protocol is 1).

5. Click **OK**.
6. Save your changes.

Configuring SNMP Responses

Introduction

You can configure Simple Network Management Protocol (SNMP) notification responses for connection, security, and user-defined events that pull certain values and send them to an SNMP manager.

How SNMP works

Simple Network Management Protocol (SNMP) is a set of protocols used for managing networks. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to SNMP management applications, such as HP OpenView. SNMP agents only communicate with SNMP management applications located in the same community. A community is set by the user for basic authentication purposes.

About the ISS MIB file

To display the ISS-assigned Event Name in SNMP trap messages, you can import or compile the ISS MIB file (`iss.mib`) into an SNMP management application such as Hewlett-Packard OpenView. The ISS MIB file defines the format of ISS SNMP traps, and is used by your management application to provide translations of the numeric Object Identifiers (OIDs) contained in the trap messages. You can download the iss.mib file from the ISS Download Center at http://www.iss.net/download/. For more information about using the SNMP management application, see the SNMP management application software documentation.

Adding SNMP responses

To add SNMP responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **SNMP** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a meaningful name for the response. **Tip**: This is the name that appears when you select responses for events, so you should give the response a name that allows users to easily identify what they are selecting.
Manager	Type the server IP address where the SNMP Manager is running. The SNMP Host must be accessible to the appliance to send SNMP traps.
Community	Type a valid name (public or private) used to authenticate with the SNMP agent.

5. Click **OK**.
6. Save your changes.

Working with SNMP responses

To edit, copy, or remove SNMP responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **SNMP** tab.
3. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the SNMP tab by double-clicking the item you want to configure. 1. Select the response, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the response, and then click **OK**.
Copy	1. Select the response, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the response as needed, and then click **OK**.
Remove	1. Select the response. 2. Click the **Remove** icon.

4. Save your changes.

Configuring User Specified Responses

Introduction

You can configure user-specified responses to events, such as executing an application or script.

Using executables or shell scripts

For user-specified responses, you can use a Linux binary or shell script, including any command-line options or arguments (such as event name or source address).

After you create the response, you must manually copy the executable to the appliance. You can define as many different user-specified responses as needed, but the appliance can only execute one response for a specific event. To run a series of executables, you must place all commands in a shell script that the appliance can run.

Adding user specified responses

To add user specified responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **User Specified** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a meaningful name for the response. **Tip**: This name appears when you select responses for events, so you give the response a name that allows users to easily identify what they are selecting.
Command	Type a command associated with the response.
Sensor Parameters	Expand the list, select a parameter, and then click **Add**. Repeat this step for each parameter you want to add to the response. You can click **Move Up** or **Move Down** to place the parameters in the appropriate order.

5. Click **OK**.
6. Save your changes.

Working with user specified responses

To edit, copy, or remove user specified responses:

1. Do one of the following:
   - In Proventia Manager, select **Responses**.
   - In SiteProtector, select **Response Objects**.
2. Select the **User Specified** tab.

3. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the User Specified tab by double-clicking the item you want to configure. 1. Select the response, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the response, and then click **OK**.
Copy	1. Select the response, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the response as needed, and then click **OK**.
Remove	1. Select the response. 2. Click the **Remove** icon.

4. Save your changes.

Chapter 8

Working with Security Events

Overview

Introduction

This chapter describes how to configure security events and response filters. These help you create a security policy that determines how the appliance responds to and reports security events that occur on the network.

In this chapter

This chapter contains the following topics:

Topic	Page
Configuring Protection Domains	78
Configuring Security Events	80
Assigning Multiple Security Events to a Protection Domain	83
Viewing Security Event Information	84
Configuring Response Filters	86
Viewing Response Filter Information	90

Configuring Protection Domains

Introduction

Protection domains let you define security policies for different network segments monitored by a single appliance. Protection domains act like virtual sensors, as though you had several appliances monitoring the network. You can define protection domains by ports, VLANs, or IP address ranges.

When to use

You use protection domains when you want to monitor groups of different network segments from a single appliance using global policies that centralize intrusion prevention.

Use protection domains as follows:

- to define and apply multiple protection domains to a single appliance
- to apply multiple policies to a single appliance, which lets you tune the responses to specific network traffic on one or more networks

Protection domains and security events

The appliance always uses a global security policy. This means that the appliance handles security events in the same manner for all areas of the network. The appliance always uses this single global policy to handle security events, unless you define protection domains and edit security event policies to suit each domain.

Once you have configured protection domains, you use them in conjunction with security policies that handle security events occurring on the network.

You can create specific security policies for specific protection domains, or you can tweak the global policy for specific domains as you see fit. These policies tell the appliance what properties signal an event and how to respond if the event occurs.

Note: Certain Flood and Sweep signatures are not supported with user-defined Protection Domains. These attacks generally affect multiple targets, which are potentially spread across Protection Domains. You should enable these signatures for the Global Protection Domain so they are reported correctly.

Adding protection domains

To add or change protection domains:

1. On the **Protection Domains** page, click **Add**.
2. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select this check box to enable the protection domain.
Protection Domain Name	Type a descriptive name for the domain.
Comment	Type a unique description for the domain.

Setting	Description
Adapter	Select an appliance monitoring adapter or a list of monitoring adapters. **Note**: The appliance ignores port configurations that do not apply to the specific appliance. For example, the appliance may only allow you to configure two adapter ports if it only has two ports, even though there are additional ports available for configuration.
VLAN Range	Type the range of virtual LAN tags or leave blank.
IP Address Range	Type the range of source and destination IP addresses.

3. Click **OK**.
4. Save your changes.

Working with protection domains

To edit, copy, or remove protection domains:

1. Select **Protection Domains**.
2. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Protection Domains page by double-clicking the item you want to configure. 1. Select the domain, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the domain, and then click **OK**.
Copy	1. Select the domain, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the domain as needed, and then click **OK**.
Remove	1. Select the domain. 2. Click the **Remove** icon.

3. Save your changes.

Configuring Security Events

Introduction

The Security Events page lists hundreds of attacks, audits, and security events. A security event is network traffic with content that can indicate an attack or other suspicious activity. These events are triggered when the network traffic matches one of the events in the active security policy, which you can edit to meet the network's needs.

About the global protection domain

Notice that all events are listed under the global protection domain. The appliance always uses a global security policy, which means that it handles security events in the same manner for all areas of the network. Configure events at the global level that you want to apply across all segments in the network. To configure security policies for specific segments on the network, create protection domains for each segment.

Adding security events to a protection domain

To add security events:

Note: The settings that appear in this procedure correspond to the columns that appear on the Security Events tab.

1. Select **Security Events**.
2. On the **Security Events** tab, click **Add**.
3. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select the check box to enable the event as part of the security policy.
Protection Domain	If you have protection domains configured, select one from the list. You can only apply one event to one domain at a time; to configure this event for another domain, copy and rename the event, and then assign it to the other domain. **Note**: The protection domain appears as "Global" in the list if you have not configured (or are not using) protection domains.
Attack/Audit	If you are creating a custom event, this area is unavailable. If you are editing an event in the list, this area displays whether this is an audit or attack event. • Audit events match network traffic that seeks information about the network. • Attack events match network traffic that seeks to harm the network.
Tag Name	Type a unique descriptive name for the event. If you are editing an existing event, the event name appears. Click **Signature Information** to view a brief description of the event.
Severity	Select a severity level for the event: Low, Medium, or High.
Protocol	Type the protocol for the event. For existing events, this setting displays the protocol type and is read-only.
Ignore Events	Select this check box to have the appliance ignore events that match the criteria set for this event.

Setting	Description
Display	Select how you want to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to block the attack by dropping packets and sending resets to TCP connections.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory on the appliance.
Responses	To enable responses, select one of the following tabs: • **Email**. Select an email response from the list. • **Quarantine**. Select one or more check boxes to enable quarantine responses. • **SNMP**. Select an SNMP response from the list. • **User Defined**. Select one or more check boxes to enable user-defined responses. **Note**: You can click **Edit** to change the properties of any response in the list. Fore more information, see “Configuring Responses” on page 67.
XPU	Displays the XPU in which the vulnerability check was released. This setting is read-only.
Event Throttling	Type an interval value in seconds. At most, one event that matches an event is reported during the interval you specify. A value of 0 (zero) disables event throttling.
Check Date	Displays the month and the year the vulnerability check was created. This setting is read-only.
Default Protection	Displays the default protection setting for the event, such as “Block.” This setting is read-only.
User Overridden	If you are creating a new event, this check box is enabled by default to indicate a custom event. In the list on the Security Events tab, this item appears as checked for both custom events and existing events that you have edited. This setting is read-only.

4. Click **OK**.
5. Save your changes.

Working with security events

To edit, copy, or remove security events:

1. Select **Security Events**.
2. Select the **Security Events** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Security Events tab by double-clicking the item you want to configure. 1. Select the event, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the event, and then click **OK**.
Copy	**Tip**: Copying and pasting security events is much easier if you group and filter the events first. See "Grouping security events" on page 84 or "Viewing security events" on page 85 for more information. 1. Select the event, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the event as needed, and then click **OK**.
Remove	1. Select the event. 2. Click the **Remove** icon. **Important**: You can only remove custom events. If you select a predefined event that you have edited and click Remove, the event is reset to its default settings and remains in the list.

3. Save your changes.

Editing multiple security events

To edit multiple security events:

1. Select **Security Events**.
2. On the **Security Events** tab, do one of the following:
   - To select multiple events, press CTRL, and then select each event.
   - To select a range of events, press SHIFT, and then select the first and last events in the range.
3. Click **Edit**.

   Every item you edit is changed for every selected event.

   A blue triangle icon appears next to any item in the selected events that has a different value. If you change the value of a field with this icon, the value changes to the new setting for all selected events and the blue triangle icon no longer appears next to the field.

   For example, if you select to edit two events and one has blocking enabled and the other does not, a blue triangle appears next to Block. If you enable the block response on the one that was originally disabled, then both events have blocking enabled, and the blue triangle disappears.
4. Click **OK**.
5. Save your changes.

Assigning Multiple Security Events to a Protection Domain

Introduction

Once you have configured the protection domains, you can assign multiple security events to them. The saves you time when you are configuring the security policy for each protection domain on the network.

Procedure

To assign a multiple security events to a protection domain:

1. Select **Security Events**.
2. On the **Security Events** tab, select the events as follows:
   - To select multiple events, press the CTRL key, and then select each event.
   - To select a range of events, press the SHIFT key, and then select the first and last events in the range.
3. Click **Copy**.
4. Click **Paste**.
5. Select all entries with the red X icon, and then click **Edit**.
6. Select the **Protection Domain** that you want to assign to the selected events.
7. Edit any additional settings.

   For more information, see “Adding security events to a protection domain” on page 80.
8. Click **OK** to return to the Security Events page.
9. Save your changes.

Viewing Security Event Information

Introduction

The Security Events tab lists hundreds of attacks, audits, and security events. You can customize how events appear to make viewing and searching easier.

About filters and regular expressions

Security events filters use regular expressions to limit the number of events displayed.

Regular expressions (also known as regex) are sets of symbols and syntax that you can use to search for text that matches the patterns you specify. If you have ever performed a wildcard search, you have used regular expressions.

At the most basic level, the following wildcard search types are supported:

Search value...	Returns...
*	all events
http*	all events that begin with “http”
*http	all events that end in “http”
http	all events that contain “http”

Table 31: *Sample search values for regular expressions*

Regular expressions search all columns in the Security Events list. If you search for http*, for example, the search returns all events that match the http protocol column *and* all events that begin with http.

Selecting columns to display

To select columns to display:

1. Select **Security Events**.
2. On the **Security Events** tab, click **Select Columns**.
3. Select the check box next to the columns that you want to appear.
4. Click **OK**.
5. Save your changes.

Note: If you have grouped and sub-grouped events, the columns for those events no longer appear in the Security Events tab. Instead, they appear as items in a grouping tree that you can expand or collapse.

Grouping security events

To group security events:

1. Select **Security Events**.
2. On the **Security Events** tab, click **Group By**.
3. From the All Columns list, select the column by which you want to group events, and then click **Add**.

   The columns you select appear in the Group By These Columns list.
4. Repeat **Step 3** for each column by which you want to group events.

   Each column you select to group by creates a subgroup underneath the last "group" you created.

5. Click **OK**.
6. Collapse or expand the groups on the Security Events tab to view events.
7. Save your changes.

Viewing security events

To filter security events:

1. Select **Security Events**.
2. On the **Security Events** tab, select the **Filter** check box to enable filtering.
3. Click **Filter**.
4. In the **Regular Expressions** area, type the regular expression by which you want to filter. This search feature is not case-sensitive.

   Note: To use this feature, you should be familiar with how regular expressions work.
5. For each category, select the filters you want to apply. The default is *Any*, which results in the appliance searching for any result that matches the regular expression you entered.
6. Click **OK**.
7. Save your changes.

Resetting security event values

To reset security event values:

1. Select **Security Events**.
2. On the **Security Events** tab, do one of the following:
   - Reset Events. Highlight the events to reset, and then click **Remove**. Pre-defined events that you edited are restored to default values, but remain in the list. Custom events are removed from the list.
   - Reset Groups. Click **Reset Groupings**. All grouping is removed from the events.
   - Reset Filters. Clear the **Filters** check box to disable any filters you have set.
3. Save your changes.

Configuring Response Filters

Introduction

A response filter lets you refine the security policy by controlling the number of events to which the appliance responds and the number of events reported to the management console.

You use response filters to do the following:

- configure responses for security events that trigger based off network criteria specified in the filter
- reduce the number of security events an appliance reports to the console

For example, if you have hosts on the network that are secure and trusted or hosts that you want the appliance to ignore for any other reason, you can use a response filter with the IGNORE response enabled.

Attributes of response filters

Response filters have the following configurable attributes:

- adapter
- virtual LAN (VLAN)
- source or target IP address
- source or target port number (all ports or a port associated with a particular service) or ICMP type/code (one or the other will be used)

Filters and other events

When the appliance detects traffic that matches a response filter, the appliance executes the responses specified in the filter. Otherwise, the appliance executes the responses as specified in the event itself.

Note: If a security event is disabled, its corresponding response filters are also disabled.

Response filter order

The response filters follow rule ordering. For example, if you add more than one filter for the same security event, the appliance executes the responses for the first match. The appliance reads the list of filters from top to bottom.

Adding response filters

To add response filters:

Note: The settings that appear in this procedure correspond to the columns that appear on the Response Filters tab.

1. Select **Security Events**.
2. Select the **Response Filters** tab.
3. Click **Add**.

4. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	The filter is enabled by default. To disable the filter, clear the check box.
Protection Domain	Select the protection domain for which you want to set this filter. **Note**: For a response filter to be active, the corresponding security event must be enabled for the protection domain you specify here.
Event Name	Displays a truncated event name. Click the button to add events. **Tip**: You can add multiple events at one time. Use the filter settings to sort through the list.
Event Name Info	Displays additional information about the event, if necessary. This setting is read-only.
Comment	Type a unique description for the event filter.
Severity	Select an event severity level to filter by: high, medium, or low.
Adapter	Select the appliance port(s) on which the response filter will be applied or leave all selected. **Note**: The appliance ignores port configurations that do not apply to the specific appliance. For example, the appliance may only allow you to configure two adapter ports, even though there are additional ports available for configuration.
VLAN	Type the range of virtual LAN tags where the response filter will be applied or leave empty.
Event Throttling	Type an interval value in seconds. At most, one event that matches an event is reported during the interval you specify. A value of 0 (zero) disables event throttling.
Ignore Events	Select this check box to have the appliance ignore events that match the criteria set for this event.
Display	Select how to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to block the attack by dropping packets and sending resets to TCP connections.
ICMP Type/Code	Type ICMP types or codes, or click **Well Known** to select often-used types and codes.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory.

Setting	Description
Responses	To enable responses, select one of the following tabs: • **Email**. Select an email response from the list. • **Quarantine**. Select one or more check boxes to enable quarantine responses. • **SNMP**. Select an SNMP response from the list. • **User Defined**. Select one or more check boxes to enable user-defined responses. **Note**: Click **Edit** to change the properties of any response in the list. For more information, see "Configuring Responses" on page 67.
IP Address and Port	For the Source and/or Target IP addresses or ports you want to filter by, complete or change the following settings as listed in Step 5.

5. Complete the following IP Address and Port settings as indicated in the following table.

Setting		Description
Address	Not	Select this check box to exclude addresses you specify.
	Any	Select this option to include all addresses.
	Single Address	Select this option to filter on one address, and then type the **Address**.
	Address Range	Select this option to filter on an address range, and then type the first and last addresses in the **Range**.
	Network Address/# Network Bit (CIDR)	Select this option to include an IP address on a subnet. Type the IP address and mask. The mask is the network identifier, and is a number from 1 to 32; for example: 128.8.27.18 / 16.
Port	Not	Select this check box to exclude ports you specify.
	Any	Select this option to include all addresses.
	Single Port	Select this option to include a single port, and then type the **Port** number.
	Port Range	Select this option to include a port range, and then type the first and last address in the **Range**.

6. Click **OK**.
7. Save your changes.

Changing the order of response filters

To change the order of response filters:

1. Select **Security Events**.
2. Select the **Response Filters** tab.
3. Select an entry, and then click the **Up** or **Down** icons to move the filter.
4. Save your changes.

Working with response filters

To edit, copy, or remove response filters:

1. Select **Security Events**.
2. Select the **Response Filters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Response Filters tab by double-clicking the item you want to configure. 1. Select the filter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the filter, and then click **OK**.
Copy	1. Select the filter(s), and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the filter as needed, and then click **OK**.
Remove	1. Select the filter(s). 2. Click the **Remove** icon.

3. Save your changes.

Viewing Response Filter Information

Introduction

The Response Filters tab lists response filters you have defined to control how security events are reported to the management console.

Selecting columns to display

To select columns to display:

1. Select **Security Events**.
2. Select the **Response Filters** tab.
3. Click **Select Columns**.
4. Select the check box next to the columns that you want to appear on the tab.
5. Click **OK**.
6. Save your changes.

Note: If you have grouped and sub-grouped filters, the columns for those events no longer appear in the Response Filters tab. Instead, they appear as items in a grouping tree that you can expand or collapse.

Grouping response filters

To group response filters:

1. Select **Security Events**.
2. Select the **Response Filter**s tab.
3. Click **Group By**.
4. From the **All Columns** list, select the column by which you want to group filters, and then click **Add**.

   The columns you select appear in the Group By These Columns list.
5. Repeat Step 4 for each column by which you want to group filters.

   Each column you select to group by creates a subgroup underneath the last "group" you created.
6. Click **OK**.
7. Collapse or expand the groups on the Response Filters tab to view filters.
8. Save your changes.

Changing response filters view

To filter response filters:

1. Select **Security Events**.
2. Select the **Response Filter**s tab.
3. Select the **Filter** check box to enable filtering.
4. Click **Filter**.

   For each category, select the filters you want to apply. The default is Any, which results in the appliance searching for any result for that category.
5. Click **OK**.
6. Save your changes.

Chapter 9

Configuring Other Intrusion Prevention Settings

Overview

Introduction

This chapter describes how to configure and manage other intrusion prevention settings, such as user-defined events, connection events, and OpenSignature events. It also discusses how to manage quarantined intrusions, view global tuning parameters for the appliance, and monitor X-Force blocking.

In this chapter

This chapter contains the following topics:

Topic	Page
Managing Quarantined Intrusions	92
Configuring Connection Events	93
Configuring User-Defined Events	97
User-Defined Event Contexts	100
Regular Expressions in User-Defined Events	105
Viewing User Defined Event Information	107
Configuring OpenSignature	108
Configuring Global Tuning Parameters	110
Configuring X-Force Default Blocking	112

Managing Quarantined Intrusions

Introduction

The Quarantined Intrusions page shows quarantine rules dynamically generated in response to detected intruder events. When quarantine response is enabled, the rules specify the packets to block and the length of time to block them. They prevent worms from spreading, and deny access to systems infected with backdoors or trojans.

Important: You can view or remove Quarantined Intrusions only through Proventia Manager.

Quarantine rules columns

You can view the following information on the Quarantine Rules tab:

Note: An asterisk * in a field means that the rule is ignoring that part of the rule.

Field	Description
Source IP	Source IP address of packets to block
Source Port	Source port number of packets (if protocol is 6 or 17) to block
Dest IP	Destination IP address of packets to block
Dest Port	Destination port number of packets (if protocol is 6 or 17) to block
ICMP Type	ICMP type of packets (if protocol is 1) to block.
ICMP Code	ICMP code number of packets (if protocol is 1) to block
Protocol	IP protocol of the rule (ICMP=1, TCP=6, UDP=17)
Expiration Time	Rule's expiration time
Block Percentage	Percentage of packets that are dropped (use values less than 100% to lessen the impact of some denial-of-service attacks)

Table 32: *Quarantine rules columns*

Viewing quarantine rule details

To view quarantine rule details:

1. In Proventia Manager, select **Intrusion Prevention→Quarantined Intrusions**.
2. On the Quarantined Rules tab, select a rule, and then click **Display**.
3. Click **OK** to return to the Quarantined Rules tab.

Removing quarantine rules

To remove quarantine rules:

1. In Proventia Manager, select **Intrusion Prevention→Quarantined Intrusions**.
2. Select the quarantine rule from the Rules table, and then click **Remove**.
3. Save your changes.

Configuring Connection Events

Introduction

Connection events are user-defined notifications of open connections to or from particular addresses or ports. They are generated when the appliance detects network activity at a designated port, regardless of the type of activity, or the content of network packets exchanged.

The Connection Events page lists pre-defined connection events for different connection types, such as WWW, FTP, or IRC. Use this page to customize these events or to create your own events to cover the traffic you need to monitor.

For example, you can define a signature that causes a connection event to alert the console whenever someone connects to the network using FTP.

Note: The connections are always registered against the destination port you specify, so to monitor an FTP connection, you must use the FTP port. One entry per connection is sufficient for traffic in each direction.

How connection events work

Connection events occur when network traffic connects to the monitored network through a particular port, from a particular address, with a certain network protocol. The appliance detects these connections using packet header values. Connection events do not necessarily constitute an attack or other suspicious activity, but they are network occurrences that might interest a Security Administrator.

Note: Connection events do not monitor the network for any particular attack signatures. You use security events to monitor for these types of attacks. See "Configuring Security Events" on page 80 for more information.

About removing connection events

You can remove any connection event from the list. However, if you edited a pre-defined connection event and now decide you want to remove it, be aware that the event is not returned to its pre-defined state. The event is removed from the list entirely. If you want to use this event again in the future, it will no longer be available.

Consider disabling the event and keeping it in the list. This way, if you want to use it again at another time, the event is still available to you in some form.

Adding connection events

To add connection events:

Note: The settings in this procedure correspond to the columns that appear on the Connection Events page.

1. On the **Connection Events** page, click **Add**.
2. Complete the settings as indicated in the following table.

Setting	Description
Enabled	The event is enabled by default. If necessary, clear the check box to disable the event.
Event Name	Type a unique descriptive name for the event. If you are editing a pre-defined event, the name appears here as read-only.

Setting	Description
Comment	Type a unique description for the event.
Severity	Select a severity level for the event: Low, Medium, or High.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack is reported during the interval you specify. A value of 0 (zero) disables event throttling.
Protocol	Type the protocol for the event. If you select the ICMP protocol, type the ICMP types or codes for either side of the packet, or click **Well Known** to select often-used types and codes.
Display	Select how you want to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to block the attack by dropping packets and sending resets to TCP connections.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory.
IP Address and Port	See Step 3.
Responses	See Step 4.

3. As needed, complete the following **IP Address and Port** settings as indicated in the following table.

Setting		Description
Address	Not	Select this check box to exclude addresses you specify.
	Any	Select this option to include all addresses.
	Single Address	Select this option to filter on one address, and then type the **Address**.
	Address Range	Select this option to filter on an address range, and then type the first and last addresses in the **Range**.
	Network Address/# Network Bit (CIDR)	Select this option to include an IP address on a subnet. Type the IP address and mask. The mask is the network identifier, and is a number from 1 to 32; for example: 128.8.27.18 / 16.
Port	Not	Select this check box to exclude ports you specify.
	Any	Select this option to include all addresses.
	Single Port	Select this option to include a single port, and then type the **Port** number.
	Port Range	Select this option to include a port range, and then type the first and last address in the **Range**.

4. As needed, complete the following Response settings as indicated in the following table. Click **Edit** to change the properties of a response in the list. For more information, see "Configuring Responses" on page 67.

Response	Description
Email	Select an email response from the list.
Quarantine	Select one or more check boxes to enable quarantine responses.
SNMP	Select an SNMP response from the list.
User Defined	Select one or more check boxes to enable user-defined responses.

5. Click **OK**.
6. Save your changes.

Viewing connection events

To filter connection events:

1. On the **Connection Events** page, select the **Filter** check box to enable filtering.
2. Click **Filter**.
3. For each category, select the filters you want to apply.

   By default, all filters are set to *Any*, which results in the appliance searching for any result for that category.
4. Click **OK**.
5. Save your changes.

Working with connection events

To edit, copy, or remove connection events:

1. On the **Connection Events** page, do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Connection Events page by double-clicking the item you want to configure. 1. Select the event, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the event, and then click **OK**.
Copy	1. Select the event, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the event as needed, and then click **OK**.
Remove	1. Select the event. 2. Click the **Remove** icon. See "About removing connection events" on page 93 for more information.

2. Save your changes.

Configuring User-Defined Events

Introduction

Enabled events in a policy determine what an appliance detects. You create user-defined events around contexts, which basically specify the type and part of a network packet you want the appliance to scan for events.

About the global protection domain

Notice that all events are listed under the global protection domain. The appliance always uses a global policy, which means that it handles events in the same manner for all areas of your network. You should configure events at the global level that you want to apply across all segments in your network. If you want to configure policies for specific segments on your network, you should create protection domains for each segment. See "Configuring Protection Domains" on page 78 for more information.

Note the following:

- If you have two user-defined events with the same name, one assigned to the global protection domain and one assigned to a custom protection domain, and the event is triggered on the appliance, only the event assigned to the custom domain generates an alert. In this case, the custom domain always takes precedence over the global domain.
- If you have two user-defined events that are the same but have different names, when one event is triggered, each events generates its own alert. In this case, neither event takes precedence.

Important: The appliance considers two events with the same name the same event, even if their context or query strings differ.

Adding user-defined events

To add user-defined events:

Note: The settings listed in this procedure correspond to the columns that appear on the User Defined Events page.

1. On the **User Defined Events** page, click **Add**.
2. Complete the settings as indicated in the following table.

Setting	Description
Enabled	The event is enabled by default. To disable it, clear the check box.
Name	Type a unique name for the event.
Protection Domain	If you have protection domains configured, select one from the list. You can only apply one event to one domain at a time; to configure this event for another domain, copy and rename the event, and then assign it to the other domain. **Note**: The protection domain appears as "Global" in the list if you have not configured (or are not using) protection domains.
Comment	Type a unique description for the event.
Severity	Select an event severity level to filter by: high, medium, or low.

Setting	Description
Context	Select the type and part of the network packet that the appliance should scan. For more information, see “User-Defined Event Contexts” on page 100.
Search String	Type the text string in the packet (context) that determines whether an event matches this signature. You can use wildcards and other expressions in strings. For more information, see “Regular Expressions in User-Defined Events” on page 105.
Event Throttling	Type an interval value in seconds. At most, one event that matches an attack is reported during the interval you specify. A value of 0 (zero) disables event throttling.
Display	Select how to display the event in the management console: • **No Display**. Does not display the detected event. • **WithoutRaw**. Logs a summary of the event. • **WithRaw**. Logs a summary and the associated packet capture.
Block	Select this check box to block the attack by dropping packets and sending resets to TCP connections.
Log Evidence	Select this check box to log the packet that triggered the event to the /var/iss/ directory.
Responses	To enable responses, select one of the following tabs: • **Email**. Select an email response from the list. • **Quarantine**. Select one or more check boxes to enable quarantine responses. • **SNMP**. Select an SNMP response from the list. • **User Specified**. Select one or more check boxes to enable user-defined responses. **Note**: Click **Edit** to change the properties of any response in the list. For more information, see “Configuring Responses” on page 67.

3. Click **OK**.

   The event appears at the bottom of the list.

4. Save your changes.

Working with user-defined events

To edit, copy, or remove user-defined events:

1. On the **User Defined Events** page, do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the User Defined Events page by double-clicking the item you want to configure. 1. Select the event, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the event, and then click **OK**.
Copy	1. Select the event, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the event as needed, and then click **OK**.
Remove	1. Select the event. 2. Click the **Remove** icon.

2. Save your changes.

User-Defined Event Contexts

Introduction

When you create a user-defined event signature, you select a context that tells the appliance the type and particular part of a network packet to monitor for events. After you specify the context, you add a string that tells the appliance exactly what to look for when it scans the packet. See "Regular Expressions in User-Defined Events" on page 105 for more information.

For example, the email_subject context configures the appliance to monitor the subject line of email packets (messages).

DNS_Query context

Most programs use domain names to access resources on the Internet. These programs search for the DNS name on a server to determine the specific IP of an Internet resource. Use the DNS_Query context to monitor access to particular sites or classes of sites without knowing specific IP addresses.

- **Monitors**

  The DNS_Query context monitors the DNS name in DNS query and DNS reply packets over UDP and TCP. The appliance compares the information in the String box to the expanded (human-readable) version of the domain name in these packets.

  If a user accesses a site directly using an IP address, the DNS lookup does not occur, and the appliance cannot detect the event.

  To monitor for a particular URL, remember that the domain name is only the first element. For example, //www.cnn.com is the first element in http://www.cnn.com/stories. Use the URL_Data context (see "URL_Data context" on page 103) to detect the rest of the URL.

- **Examples**

  You could use the DNS_Query context along with a string value of www.microsoft.com to monitor users accessing the Microsoft Web site.

  If you are concerned about users on your site accessing hacker-related materials on the Internet, you could monitor access to domains such as the following:

  - hackernews.com
  - rootshell.com

Email_Receiver context

Use the Email_Receiver context to monitor incoming or outgoing email to a particular recipient.

- **Monitors**

  The Email_Receiver context monitors the receiver address part of the email header using the SMTP, POP, IMAP protocols. When the appliance detects an event that matches a signature using the Email_Receiver context, you can determine which protocol the email used by examining the details of the event.

  Note: This context does not monitor email sent with the MAPI protocol.

- **Examples**

  If you suspect that someone is using "social engineering" to manipulate certain employees, you can monitor inbound email to those employees' addresses and log the source IPs. Or if you suspect someone is leaking proprietary information within your company to a particular outside email address, you could track email to that address.

Email_Sender context

Use the Email_Sender context to monitor incoming or outgoing email from a particular recipient.

- **Monitors**

  The Email_Sender context monitors the sender address part of the email header using the SMTP, POP, IMAP protocols. When the appliance detects an event that matches a signature using the Email_Sender context, you can examine the details of the event to determine which protocol the email used.

  Note: This context does not monitor email sent with the MAPI protocol.

- **Examples**

  Use the Email_Sender context to detect instances of social engineering or other employee manipulation (inbound) or to detect information leaks from your company (outbound).

Email_Subject context

Use the Email_Subject context to monitor the subject line of email.

- **Monitors**

  The Email_Subject context monitors the subject line in the email header of messages using the SMTP, POP, and IMAP protocols.

  Note: This context does not monitor email sent with the MAPI protocol.

- **Examples**

  You can create signatures to detect information leaks by monitoring for important project names or file names.

  You can also use Email_Subject to detect viruses, such as the I LOVEYOU virus.

  Tip: Because viruses and other attacks have developed programs that systematically change the subject line, use the Email_Content context to track these virus types.

File_Name context

Use the File_Name context to monitor who accesses sensitive files over the network in your organization.

- **Monitors**

  The File_Name context detects when someone (or a program) attempts to remotely read a file or write to a file with any of the following protocols:

  - TFTP
  - FTP
  - Windows file sharing (CIFS or Samba)
  - NFS

  Note: NFS can open files without directly referencing the file name. Using this context to monitor NFS access to a file may not be 100% effective.

- **Example**

  When the Explorer worm of 1999 propagated over a Windows network, it attempted to write to certain files on remote Windows shares. With a worm like this, you can monitor for attempts to access files and stop the worm from propagating locally.

News_Group context

Use the News_Group context to monitor the names of news groups that people at your company access.

- **Monitors**

  The News_Group context monitors people accessing news groups using the NNTP protocol.

- **Example**

  You can use the context to detect subscriptions to news groups, such as hacker or pornography groups, that are inappropriate according to your company's Internet usage policy.

Password context

Use the Password context to identify passwords passed in clear text over the network. When a password is not encrypted, an attacker can easily steal it by monitoring traffic with a sniffer program from another site.

- **Monitors**

  The Password context monitors programs or users sending passwords in clear text using the FTP, POP, IMAP, NNTP or HTTP protocols.

  You can also use the Password context to do the following:

  - monitor compromised accounts to gain forensic data
  - monitor the accounts of terminated employees
  - detect the use of default passwords

  Note: This context does not monitor encrypted passwords.

- **Examples**

  Monitoring compromised accounts: After cancelling a compromised account, you can create a signature to monitor outside attempts to use it and find the person that accessed the compromised data.

  Monitoring terminated employee accounts: Add searches for terminated employees' passwords to detect unauthorized remote access attempts to their closed accounts.

  Detecting the use of default passwords: Set up signatures to look for default passwords relevant to your site to detect attackers probing for common vulnerabilities.

  Note: The X-Force database contains many records detailing the names of such accounts. For more information about default passwords, look up passwords in the X-Force database at http://xforce.iss.net.

- **Using this signature with Internet Scanner**

  If you scan the network using Internet Scanner, a signature using this context to check for default passwords may detect many instances of this event in response to a password scan.

SNMP_Community context

Use the SNMP_Community context to monitor the use and possible abuse of SMNP community strings.

- **Monitors**

  The SNMP_Community context monitors any packet containing an SNMP community string. An SNMP community string is a clear text password in an SNMP message. This password authenticates each message. If the password is not a valid community name, then the message is rejected.

  If an unauthorized person gains knowledge of your community strings, that person could use that information to retrieve valuable configuration data from your equipment or even to reconfigure your equipment.

  Important: ISS strongly recommends that you use highly unique community strings and that you reconfigure them periodically.

- **Examples**

  Detecting people trying to use old strings: If you change the SNMP community strings, create a signature using this context to have the appliance search for people trying to use the old strings.

  Detecting the use of default strings: The X-Force database contains information about several vulnerabilities involving default community strings on common equipment. Attackers can attempt to access to your equipment by using these default passwords. To have the appliance detect this activity, create signatures using this context to monitor for the default passwords relevant to the equipment at your site. These signatures can detect attackers attempting to probe for these common vulnerabilities.

  Reference: For more information about default passwords, look up SNMP in the X-Force database at http://xforce.iss.net.

- **Using this signature with Internet Scanner**

  If you scan your network using Internet Scanner, a signature using this context to check for SNMP community strings may detect many instances of this event in response to a SNMP scan.

URL_Data context

Use the URL_Data context to monitor various security issues or policy issues related to HTTP GET requests. An HTTP GET request occurs when a client, such as a Web browser, requests a file from a Web server. The HTTP GET request is the most common way to retrieve files on a Web server.

- **Monitors**

  The URL_Data context monitors the contents of a URL (minus the domain name or address itself) for particular strings, when accessed through an HTTP GET request.

  Note: This context does not monitor the domain name associated with an HTTP GET request.

- **Example**

  Use this context to have the appliance monitor for attacks involving vulnerable CGI scripts. ISS Advisory #32, released on August 9, 1999, describes how to use this context to search for an attempt to exploit a vulnerability in a Microsoft Internet Information Server component.

  Reference: For more information, see Vulnerabilities in Microsoft Remote Data Service at http://xforce.iss.net/alerts/advise32.php.

You could also use this context to generically search whether employees using computers to access company-banned sites, such as pornography sites.

User_Login_Name context

Use the User_Login_Name context to detect user names exposed in plain text during authentication requests. This context works for many protocols, so you can use it to track attempts to use a particular account no matter what protocol the attacker uses.

- **Monitors**

  The User_Login_Name context monitors for plain text user names in authentication requests using the FTP, POP, IMAP, NNTP, HTTP, Windows, or R* protocols.

- **Example**

  Use this context to track attempts to use compromised accounts or if you suspect recently dismissed employees have attempted to access their old accounts online. If you know the account named "FredJ" was compromised in an attack, configure a signature using this context to search for attempts to access the account.

User_Probe_Name context

Use the User_Probe_Name context to identify attempts to access to computers on your network using default program passwords.

- **Monitors**

  The User_Probe_Name context monitors any user name associated with FINGER, SMTP, VRFY, and SMTP EXPN. An attacker can use these default accounts to access to your servers or other computers in the future.

- **Example**

  Like the Password and SNMP_Community contexts, you can use the X-Force database to build a list of default accounts and passwords relevant to the systems and software on your network.

  Reference: For more information about default passwords, look up SNMP in the X-Force database at http://xforce.iss.net.

Regular Expressions in User-Defined Events

Introduction

Regular expressions (strings) are a combination of static text and variables the appliance uses to detect patterns in the contexts (network packets) you specify for user-defined event signatures. Use regular expressions when you create user-defined event signatures if you need the appliance to detect more than a single static text string.

Regular expression library

The appliance uses a custom ISS regular expression library called Deterministic Finite Automata or DFA regular expression.

Changing the order of precedence

Use parentheses in these regular expressions to offset the standard order of precedence.

The natural order of precedence would interpret 4+2*4 as 12, because in the natural order of precedence, multiplication takes precedence over addition. However, you can use parentheses to change this precedence. For example, if you use (4+2)*4, the answer would be 24 instead of 12. This example describes a mathematical use of the order of precedence, but many other non-numerical uses exist.

Reference: For more information about the order of precedence or other information about using regular expressions, see *Mastering Regular Expressions: Powerful Techniques for Perl and Other Tools (O'Reilly Nutshell)* by Jeffrey E. Friedl (Editor), Andy Oram (Editor).

Regular expression syntax

You can use the following regular expression syntax in a user-defined event signature:

Meta-Character	Description
(r)	matches r
x	matches x
xr	matches x followed by r
\s	matches either a space or a tab (not a newline)
\d	matches a decimal digit
\"	matches a double quote
\'	matches a single quote
\\	matches a backslash
\n	matches a newline (ASCII NL or LF)
\r	matches a carriage return (ASCII CR)
\t	matches a horizontal tab (ASCII HT)
\v	matches a vertical tab (ASCII VT)
\f	matches a formfeed (ASCII FF)
\b	matches a backspace (ASCII BS)
\a	matches a bell (ASCII BS)
\ooo	matches the specified octal character code

Table 33: *String standard expressions*

Meta-Character	Description
\xhhh	matches the specified hexidecimal character code
.	matches any character except newline
\@	matches nothing (represents an accepting position)
“”	matches nothing
[xy-z]	matches x, or anything between y and z inclusive (character class)
[^xy-z]	matches anything but x, or between y and z inclusive • the caret must be the first character, otherwise it is part of the set literally • enter the dash as the first character if you want to include it
“text”	matches text literally without regard for meta-characters within • the text is not treated as a unit
r?	matches r or nothing (optional operator)
r*	matches zero or more occurrences of r (kleene closure)
r+	matches one of more occurrences of r (positive kleene closure)
r{m,n}	matches r at least m times, and at most n times (repeat operator)
r|l	matches either r or l (alternation operator)
r/l	matches r only if followed by l (lookahead operator)
^r	matches r only at the beginning of a line (bol anchor)
r$	matches r only at the end of the line (eol anchor)
r, l	matches any arbitrary regular expression
m, n	matches an integer
x,y,z	matches any printable or escaped ascii character
text	matches a sequence of printable or escaped ascii characters
ooo	matches a sequence of up to three octal digits
hhh	matches a sequence of hex digits

Table 33: *String standard expressions (Continued)*

Viewing User Defined Event Information

Introduction

The User Defined Events page displays all of the custom event signatures you have created for the appliance. You can control how user-defined events appear in this view, to make managing and searching events easier.

Selecting columns to display

To select columns to display:

1. On the **User Defined Events** page, click **Select Columns**.
2. Select the check box next to the columns that you want to appear.
3. Click **OK**.

   Note: If you have grouped and sub-grouped events, the columns for those events no longer appear in the User-Defined Events page. Instead, they appear as items in a grouping tree that you can expand or collapse.
4. Save your changes.

Grouping user-defined events

To group user-defined events:

1. On the **User Defined Events** page, click **Group By**.
2. From the All Columns list, select the column by which you want to group events, and then click **Add**.

   The columns you select appear in the Group By These Columns list.
3. Repeat Step 2 for each column by which you want to group events.

   Each column you select to group by creates a subgroup underneath the last "group" you created.
4. Click **OK**.
5. Collapse or expand the groups on the User Defined Events tab to view events.
6. Save your changes.

Viewing user-defined events

To filter user-defined events:

1. On the **User Defined Events** page, select the **Filter** check box to enable filtering.
2. Click **Filter**.
3. For each category, select the filters you want to apply.

   The default is *Any*, which results in the appliance searching for any result that matches the regular expression you entered.
4. Click **OK**.
5. Save your changes.

Configuring OpenSignature

Introduction

OpenSignature (formerly Trons) uses a flexible rules language to allow you to write customized, pattern-matching IDS signatures to detect specific threats that are not already preemptively covered in IPS products. This feature is integrated into the ISS Protocol Analysis Module (PAM) as a rule interpreter.

Risks associated with OpenSignature

The capabilities of custom signature development are very broad. With this flexibility comes added risk. Poorly written rules or signatures could impact sensor performance or have other consequences. Risks of using your own custom signatures include but are not limited to the following:

- unacceptable appliance performance
- throwing PAM into an infinite loop
- blocking all network traffic to a specific segment (inline mode with or without bypass)

Caution: ISS does not guarantee appliance performance if you choose to use OpenSignature. Enable this functionality at your own risk. ISS Customer Support is not available to help you write or troubleshoot custom rules for your environment. If you require assistance to create custom signatures, please contact ISS Professional Services.

OpenSignature syntax

The syntax options for each custom rule are as follows:

`<action>: alert`

`<protocol>: tcp, udp, icmp, ip`

`<IP and netmask>`: single IP address (a.b.c.d), range of IP addresses (a.b.c.d-w.x.y.z), network address using CIDR notation (a.b.c.0/24)

The Negation operator is indicated with an '!':

```
alert tcp 192.168.1.0/24
```

This means an alert prompts you when anything other than what is indicated with the '!' is used.

Important: If you have improperly formatted an OpenSignature rule, you may receive a PAM configuration error response.

Enabling the OpenSignature Parser

To enable the OpenSignature Parser:

1. Select Global Tuning Parameters.
2. On the Tuning Parameters tab, click **Add**.
3. Complete the settings as indicated in the following table:

Setting	Description
Name	Type the following to enable OpenSignature: `engine.opensignature.enabled`
Value	Type the following: `true`

4. Save your changes.

Adding or changing rules

To add or change rules:

1. On the **OpenSignature** page, click **Add**, or highlight the rule you want to edit, and then click **Edit**.

   Tip: You can edit some properties directly on the OpenSignature page by double-clicking the item you want to configure.

2. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select the check box to enable the rule.
Comments	Type a unique description for the rule.
Rule String	Type the text string that tells the appliance when an event is triggered and how to respond to the event.

3. Click **OK**.
4. Save your changes.

Configuring Global Tuning Parameters

Introduction

Global tuning parameters affect intrusion prevention settings at the group and site levels.

Use Global Tuning Parameters to configure (or tune) certain parameters and apply them globally to a group of appliances to better meet your security needs or enhance the performance of the hardware. Generally, you edit or configure global tuning parameters for groups of appliances you manage through SiteProtector, but you can view the global tuning parameters that affect a specific appliance through Proventia Manager.

You can also specify whether you want to use blocking responses recommended by ISS X-Force. While ISS recommends that you not disable X-Force blocking as a general rule, you may need to disable this option at times so that you can determine whether current suspicious activity on the network is valid, or so that you can protect against explicit threats to the network.

How global parameters differ from local parameters

Global tuning parameters differ from local tuning parameters as follows:

- Global tuning parameters are settings that affect a group of intrusion prevention appliances.
- Local tuning parameters are settings that affect a specific intrusion prevention appliance, such as network adapter card settings.

  Because local tuning parameters are specific to a particular appliance, you can configure them only at the device level.

Where applicable, local tuning parameters you have enabled take precedence over global tuning parameters.

Components you can tune

You can tune the following components on a group of appliances:

- intrusion prevention responses
- intrusion prevention security risks
- firewall
- automatic updates

See “Configuring Advanced Parameters” on page 129 for information about applying advanced parameters to a single appliance.

About advanced parameters

Advanced parameters are composed of name/value pairs. Each name/value pair has a default value.

For example, the parameter np.firewall.log is a parameter that determines whether to log the details of packets that match firewall rules you have enabled. The default value for this parameter is on.

You can edit the value of any parameter that appears in the list on the Advanced Parameters tab. If the parameter does not appear in the list, it does not mean the parameter has no default value. You simply need to add the parameter to the list with the new value.

Adding tuning parameters

To add tuning parameters:

1. Select **Global Tuning Parameters**.
2. On the **Tuning Parameters** tab, click **Add**.
3. Complete the settings as indicated in the following table.

Setting	Description
Name	Type a name for the parameter. **Example**: np.log.count
Value	Type a value according to the value type associated with the parameter: • **Boolean**. Select a value of True or False. • **Number**. Enter the appropriate number for the parameter. **Example**: 10 • **String**. Type the value for the parameter, such a log file location.
Comment	Type a unique description for the parameter. **Example**: Number of event log files.

4. Click **OK**.
5. Save your changes.

Working with global tuning parameters

To edit, copy, or remove global tuning parameters:

1. Select **Global Tuning Parameters**.
2. Select the **Tuning Parameters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Tuning Parameters tab by double-clicking the item you want to configure. 1. Select the parameter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the parameter, and then click **OK**.
Copy	1. Select the parameter, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the parameter as needed, and then click **OK**.
Remove	1. Select the parameter. 2. Click the **Remove** icon.

3. Save your changes.

Configuring X-Force Default Blocking

Introduction

When you use X-Force Default Blocking, the block response is enabled automatically for events (or signatures) that X-Force recommends.

Procedure

To configure default blocking:

1. Select **Global Tuning Parameters**.
2. Select the **X-Force Default Blocking** tab.
3. X-Force blocking is enabled by default. To disable it, clear the **Use X-Force blocking recommendations** box.
4. Save your changes.

Chapter 10

Configuring Firewall Settings

Overview

Introduction

Using rule statements, you can configure firewall rules to block attacks based on various source and destination information in the packet. In addition, you can filter out traffic you do not want to have inspected if you are not interested in seeing it.

In this chapter

This chapter contains the following topics:

Topic	Page
Configuring Firewall Rules	114
Firewall Rules Language	117
Tuning Firewall Logging	120

Configuring Firewall Rules

Introduction

You can add firewall rules to block unwanted traffic before they enter the network. You can manually add firewall rules, or you can enable the appliance to construct rules using the values you specify. This offers you greater flexibility when configuring firewall settings.

Important: Firewall rules only work when the appliance is set to inline modes. An appliance in passive mode works like a traditional sensor and is not in the direct path of the packets. In simulation mode, packets still pass through the appliance, and it describes what it would have done to the traffic in protection mode.

Use the Firewall Rules page to configure firewall rules to block attacks based on various source and target information in the packet.

Firewall rule criteria

You can define firewall rules using any combination of the following criteria:

- Adapter
- VLAN range
- Protocol (TCP, UDP, or ICMP)
- Source or target IP address and port ranges

Firewall rule order

The appliance reads the list of firewall rules from top to bottom in the order they are listed and applies corresponding actions. When a connection matches a firewall rule, further processing for the connection stops, and the appliance ignores any additional firewall rules you have set.

Example

Use the following statements to block all connections to a network segment except those destined for a specific port on a specific host:

```
adapter any IP src addr any dst addr 1.2.3.4 tcp dst port 80
```

(Action = "ignore")

```
adapter any IP src addr any dst addr 1.2.3.1-1.2.3.255
```

(Action = "drop")

The first rule allows all traffic to port 80 on host 1.2.3.4 to pass through to a Web server as legitimate traffic. All other traffic on that network segment is dropped.

If you reverse the rule order, all traffic to the segment is dropped, even the traffic to the Web server on 1.2.3.4.

Firewall rules and actions

The firewall supports several different *actions* that describe how the firewall reacts to the packets matched in the rules, or *statements*. The following Table 34defines these actions:

Rule	Description
Ignore (Permit)	Allows the matching packet to pass through, so that no further actions or responses are taken on the packet.
Protect	Packets that match this rule are processed by PAM. Enables matching packets to be processed by normal responses, such as (but not limited to) logging, the block response, and quarantine response.
Monitor	Functions as an IP whitelist. Allows to packets that match the statements bypass the quarantine response and bypass the block response. However, all other responses still apply to the packet.
Drop (Deny)	Drops the packets as they pass through the firewall. Because the firewall is inline, this action prevents the packets from reaching the target system. To the person whose packet is dropped, it appears as if the target system simply does not respond. The connection most likely makes several retry attempts, and then the connection eventually times out.
Drop and Reset	Functions in the same manner as the drop action, but sends a TCP reset to the source system. The connection terminates more quickly (because it is automatically reset) than with the drop action.

Table 34: *Firewall actions*

Adding firewall rules

To add firewall rules:

5. On the **Firewall Settings** page, click **Add**.
6. Complete the settings as indicated in the following table.

Setting	Description
Rule ID	Displays the rule's order in the list. See “Changing the order of firewall rules” on page 116 for more information.
Enabled	Select this check box to enable the rule.
Rule Comment	Type a unique description for the rule.
Log	Select whether to log details of the packets that match the rule in the Firewall log located in the /var/iss/ directory.
Action	Select a firewall action from the list. See “Firewall rules and actions” on page 115 for descriptions of each action.
Rule Type	Select a rule type from the list: • **Constructed**. Select this option to enable Proventia Manager to construct the firewall rule for you using the values you specify. • **Manually Entered**. Select this option to construct your own firewall rules. Type the **Firewall Rule** statement in the area provided. For more information, see “Firewall Rules Language” on page 117.
VLAN	Enter a range of VLAN tags.

Setting	Description
Protocol	Select a protocol from the list. If you select *Any* as the protocol for a rule, the following criteria is applied if the following conditions are met: • If you set an ICMP code, then an ICMP clause is added to the rule. • If you set a source or destination port, then both a UDP and a TCP clause are added to the rule. • If you set a Protocol Number greater than zero (0), then a protocol number clause is added to the rule. • If you do not specify any protocol settings, then an IP clause is added to the rule. The source and destination IP addresses will also be added if you have specified them. **Note**: If you set a Protocol value other than Any, the firewall rule is set to that protocol only.
IP Address and Port	Configure the source and target IP addresses and ports.

7. Click **OK**.
8. Save your changes.

Changing the order of firewall rules

To change the order of firewall rules:

1. On the Firewall Settings page, select a rule, and then click the **Up** or **Down** icons to move the rule.
2. Save your changes.

   The appliance processes the firewall rules in the order you specify.

Working with firewall rules

To edit, copy, or remove firewall rules:

1. Select **Firewall Settings**.
2. Do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Firewall Rules tab by double-clicking the item you want to configure. 1. Select the rule, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the rule, and then click **OK**.
Copy	1. Select the rule, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the rule as needed, and then click **OK**.
Remove	1. Select the rule. 2. Click the **Remove** icon.

3. Save your changes.

Firewall Rules Language

Introduction

A firewall rule consists of several statements (or clauses) that define the traffic for which the rule applies. When you manually create firewall rules for the appliance to use, you can use the syntax listed in this topic.

Firewall clauses

A firewall rule consists of several clauses chained together to match specific criteria for each packet. The clauses represent specific layers in the protocol stack. Each clause can be broken down into conditions and expressions. The expressions are the variable part of the rule in which you plug in the address, port, or numeric parameters.

You can use the following firewall clauses:

- **Adapter clause**

  Specifies a set of adapters from A through P that attaches the rule to a specific adapter. The adapter clause indicates a specific adapter where the rule is applied. The supported adapter expressions are **any** and the letters **A** through **P**. If you do not specify an adapter clause, the rule matches packets on any adapter.

  ```
  adapter <adapter-id>
  adapter A
  adapter any
  adapter A,C
  adapter A-C
  ```

- **Ethernet clause**

  Specifies either a network protocol type or virtual LAN (VLAN) identifier to match the 802.1 frame. You can use the Ethernet clause to filter 801.1q VLAN traffic or allow/deny specific types of Ethernet protocols. You can find the list of protocol types at http://www.iana.org/assignments/ethernet-numbers. Ethernet protocol constants can be specified in decimal, octal, hexadecimal, or alias notation. To make it easier to block specific types of Ethernet traffic, you can specify an alias instead of the well-known number. In some cases, the alias blocks more than one port (for example, IPX and PPPoE).

  ```
  ether proto <protocol-id>
  ether proto {arp|aarp|atalk|ipx|mpls|netbui|pppoe|rarp|sna|xns}
  ether vid <vlan-number>
  ether vid <vlan-number> proto <protocol-id>
  ```

  ```
  ether proto !arp
  ether vid 1 proto 0x0800
  ether vid 2 proto 0x86dd
  ether vid 3-999 proto 0x0800,0x86dd
  ```

- **IP datagram clause**

  Specifies the transport level filtering fields such as IPv4 addresses, TCP/UDP source or destination ports, ICMP type or code, or a specific IP protocol number. The IP datagram clause identifies the protocol that resides inside the IP datagram and the protocol-specific conditions that must be satisfied in order for the statement to match. Currently, only ICMP, TCP, and UDP conditions are supported, but you can specify filters based on any IP protocol. If you do not specify an IP datagram clause, the statement will match any IP datagram protocol.

  The first and second statements below block IP packets that match the IP address expression. The third statement below blocks IP packets that match the IP address expression. The fourth statement below blocks IP packets that match the protocol

type. The fifth statement is a combination of the first and second statements. The sixth statement is a combination of the first, second, and fourth statements.

```
1. ip src addr <IPv4-addr>
2. ip dst addr <IPv4-addr>
3. ip addr <IPv4-addr>
4. ip proto <protocol-type>
5. ip src addr <IPv4-addr> dst addr <IPv4-addr>
6. ip src addr <IPv4-addr> dst addr <IPv4-addr> proto <protocol-type>
```

Examples

```
ip addr 192.168.10.1/24
ip addr 192.168.10.0-192.168.10.255
```

Firewall conditions

TCP and UDP Conditions

You can specify TCP and UDP port numbers in decimal, octal, or hexadecimal notation. The port's value range is 0 through 65535.

```
tcp src port <TCP-UDP-port>
tcp dst port <TCP-UDP-port>
tcp dst port <TCP-UDP-port> src port <TCP-UDP-port>
udp src port <TCP-UDP-port>
udp dst port <TCP-UDP-port>
udp dst port <TCP-UDP-port> src port <TCP-UDP-port>
```

ICMP conditions

You can specify ICMP conditions in decimal, octal, or hexadecimal notation. You can find the valid number for type and code at http://www.iana.org/assignments/icmp-parameters.

```
icmp type <protocol-type>
icmp code <message-code>
icmp type <protocol-type> code <message-code>
```

Expressions

An expression describes a list of header values that must match the clause's protocol parser. Each clause is directly responsible for matching a specific layer in the protocol stack. The syntax and accept range of values is determined by the clause. The expression can be a single value, a comma separated list of values, or a range set. Currently, expressions exist to specify adapter numbers, IPv4 addresses, TCP and UDP port numbers, ICMP message type and codes, and IP datagram protocol numbers.

```
<value>
<value>, <value>
<value> - <value>
```

Expressions that begin with an exclamation marks (**!**) are called a *not-expressions*. Not-expressions will match all values except those you specify. Not-expressions that do not match any values will generate an error.

IPv4 address expression examples

The <n> can be either hex or decimal number in a range from 0 to 255. All hex numbers must have a 0x prefix. The following table lists examples.

Example	Description
n.n.n.n	Single address
n.n.n.n, n.n.n.n	Address list
n.n.n.n/<netmask>	Specific address using CIDR format; netmask value must range from 1 to 32
n.n.n.n - n.n.n.n	Address range, where first value is greater than last

Table 35: *IPv4 address syntax*

TCP/UDP ports, protocol identifiers, or numbers

The values listed for any constant must be within the fields required range; otherwise the parser will refuse the parse clause.

```
0xFFFF
65535
0, 1, 2
0 - 2
! 3 - 65535
```

Complete firewall rule examples

The following statements are examples of complete firewall rules. If you do not specify a protocol, the rule assumes and uses the **any** protocol.

- `adapter A ip src addr xxx.xxx.x.x`

  (where x is a number in the IP address)
- `adapter A ip src addr xxx.xxx.x dst addr any tcp src port 20 dst port 80`

  (where x is a number in the IP address)
- `adapter any ip src addr any dst addr xxx.xxx.xx.x`
- `adapter any ip src addr any dst addr any icmp type 8`
- `tcp`
- `adapter B icmp`
- `udp`

Tuning Firewall Logging

Introduction

Using Local Advanced Parameters, you can tune the way firewall logging behaves for the appliance. You can specify values such as the number of firewall logs, the log name, or the maximum log size.

Firewall logging parameters

You can edit the following firewall logging parameters:

Name	Description	Values
np.firewall.log	Determines whether to log the details of packets that match firewall rules that are enabled.	string Default: on
np.firewall.log.count	Number of firewall log files.	number Default: 10
np.firewall.log.prefix	Prefix of firewall log file name.	string Default: /var/iss/fw
np.firewall.log.size	Maximum size of a firewall log file in bytes.	number Default: 1400000
np.firewall.log.suffix	Suffix of firewall log file name.	string Default: .log

Table 36: *Firewall advanced parameters*

Procedure

To tune the firewall log settings:

1. Select **Local Tuning Parameters**.
2. Select the **Advanced Parameters** tab.
3. Select the parameter you want to change, and then click **Edit**.
4. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select this check box to enable the parameter.
Name	Displays the name of the parameter. **Note**: ISS recommends that you do not edit the parameter's name.
Comment	Describes the parameter. Type a new description if necessary.
Value	Edit the value for the parameter. **Note**: ISS recommends that you keep the default parameter value.

5. Click **OK**.
6. Save your changes.

Chapter 11

Configuring Local Tuning Parameters

Overview

Introduction

Local tuning parameters affect intrusion prevention settings at the device level for individual appliances. This chapter describes how to configure local tuning parameters for the appliance, such as the alert queue, the network card adapter properties, and advanced parameters.

In this chapter

This chapter contains the following topics:

Topic	Page
Configuring Alerts	122
Managing Network Adapter Cards	125
Managing the Alert Queue	128
Configuring Advanced Parameters	129
Configuring TCPReset	133

Configuring Alerts

Introduction

You can configure alert messages that notify you about appliance-related events. You can also determine what action the appliance should take when an event causes an alert, such as sending an email to the appliance administrator, or running an executable in response to the event.

Alert types

You can enable three types of sensor event alerts:

- **Error**. These alerts notify you when a sensor system error has occurred.
- **Warning**. These alerts notify you when a problem has occurred on the appliance itself.
- **Informative**. These alerts notify you about what actions users may have performed on the appliance, such as changing passwords, downloading logs, or editing a parameter.

System alerts and SNMP

Through the Configuration Menu on the appliance, you can configure the appliance to send SNMP traps in the event of system health-related events such as the following:

- no free disk space
- disk failure
- overly-high CPU usage

When the appliance detects these problems, it can send an SNMP trap to the SNMP receiver that was specified. These system-related alerts can be sent as SNMPv1 or SNMP v2c traps. See “SNMP configuration” on page 27 for information about configuring SNMP system health-related alerts.

Supported hardware alerts for G400 and G2000

You cannot send SNMP alerts on HDD failures on G400 or G2000.

To enable hardware alerts, you must log in as an administrator and enable SNMP through the SNMP Configuration menu.

The G400 supports the following hardware alerts:

- BIOS ECC Error
- BIOS Post Error
- Chassis Intrusion
- FRB Failure
- Fan Failure
- Fatal NMI
- Power supply fault
- Temperature out of range
- Voltage out of range
- System restart

Important: These hardware alerts are not supported on G2000 or EX6000.

Procedure

To configure an alert:

1. Select **Local Tuning Parameters**.
2. Select the **Alerts** tab.
3. In the area for the alert type (Sensor Error, Warning, Informative) to configure, select the **Enable** check box.
4. Select a **Priority** for the alert: Low, Medium, or High.
5. Select the **Display on console** check box to enable the alert to appear in the console.

   Note: In Proventia Manager, alerts appear on the Alerts tab. In SiteProtector, alerts appear on the Analysis tab in the Console.
6. To send an SNMP trap, complete or change settings indicated in the following table.

Setting	Description
Send SNMP Trap	Select the check box to enable the option, and then do one of the following: • To use a previously configured SNMP trap, select one from the list, and then go to Step 7. • To configure a new SNMP trap, click **Configure SNMP**.
Configure SNMP	Click **Add**, and then specify the following: • **Name**. Type the name of the SNMP trap or response. • **Manager**. Type the IP address where the SNMP Manager is running. The appliance must be able to access the SNMP Host to send SNMP traps. • **Community**. Type the appropriate community name (public or private).

7. To send an email notification, complete or change the settings as indicated in the following table.

Setting	Description
Send Email	Select the check box to enable the option, and then do one of the following: • To use a previously configured email notification, select one from the list, and then go to Step 8. • To configure a new email notification, click **Configure Email**.

Setting	Description
Configure Email	Click **Add**, and then specify the following: • **Name**. Type a meaningful name. • **SMTP Host**. Type the mail server (as a fully qualified domain name or IP address). **Note**: The SMTP Host must be accessible to the appliance to send email notifications. • **From**. Type individual or group email address(es). Separate addresses with commas. • **To**. Type individual recipient or email group(s). Separate addresses with commas. • **Subject**. Type a subject, or select Common Parameters from the list. When you select common parameters, they are populated with the corresponding event information. • **Body**. Type the message body, or select Common Parameters from the list. When you select common parameters, they are populated with the corresponding event information.

8. Save your changes.

Managing Network Adapter Cards

Introduction

You can view and manage settings for the appliance's network adapter cards.

Important: If you change any settings on this page, the appliance may lose link temporarily.

About high availability mode

The Proventia Network IPS High Availability (HA) feature enables the appliances to work in an existing high availability network environment. The appliances pass all traffic between them over mirroring links, ensuring they both see all of the traffic over the network and thus maintain state. The appliances also see asymmetrically routed traffic in order to fully protect the network. Proventia Network IPS High Availability support is limited to two cooperating appliances.

Both appliances process packets inline and block attack traffic that arrives on their inline monitoring ports, not on their interconnection/mirror ports. Both appliances also report events received on their inline monitoring ports to the management console.

For detailed information about high availability, see "Configuring Appliances for High Availability" on page 33.

Editing network adapter card properties

To edit network adapter card properties:

1. Select **Local Tuning Parameters**.
2. Select the **Adapter Management** tab.
3. Select an adapter in the list, and then click **Edit**.
4. Type a meaningful name to associate with the **Port**.

   Note: The port names correspond to the labels 1A, 1B, 2C, 2D, 3E, 3F, 4G, and 4H and so on, on the appliance. The ports are arranged as pairs of ports as follows:

   - 1A with 1B on Card1
   - 2C with 2D on Card2
   - 3E with 3F on Card3
   - 4G with 4H on Card4
5. From the **TCP Resets** drop-down, specify whether TCP reset packets should be sent through this port or through the external kill port. This option is only applicable in passive monitoring mode.

6. For the **Port/Duplex Speed Settings**, select the method the network adapter should use to determine link speed and mode.

Method	Description
Auto or Auto Negotiate	Allows two interfaces on a link to select the best common mode automatically, the moment a cable is connected. IBM ISS recommends that you use this setting unless you have to change the setting for a switch or other network device that does not support auto-negotiation, or if the auto-negotiation process is taking too long to establish a link. **Auto** is the only option available for the GX6116 appliance. It automatically links at 1 gigabit per second.
10 MB Half Duplex	Device either transmits or receives information at 10 megabits per second, but not at the same time.
10 MB Full Duplex	Device transmits information at 10 megabits per second in both directions at the same time.
100 MB Half Duplex	Device either transmits or receives information at 100 megabits per second, but not both at the same time.
100 MB Full Duplex	Device transmits information at 100 megabits per second in both directions at the same time.
1000 MB Full Duplex	Device transmits information at 1000 megabits per second in both directions at the same time.

Note: Not all connection options are available for all appliance models.

7. In the **Unanalyzed Policy** list, select one of the following options to determine how the agent processes traffic when the network is congested.

Option	Description
Forward	Forwards traffic without processing it, or fails open to traffic. When traffic levels return to normal, the agent resumes normal operation. **Note**: Always use the Forward setting when the appliance is set to inline simulation mode.
Drop	Blocks some of the traffic without processing it, or fails closed to traffic. When traffic levels return to normal, the agent returns to normal operation.

8. Set the **Propagate Link** option if the Adapter Mode is set to either inline protection or inline simulation mode. Select one of the following options:

Option	Description
Auto	Uses the most appropriate link setting, based on how the network segment is configured. The Propagate Link setting behaves as “True” if the appliance is in Inline Protection, Inline Simulation, or HA mode. It behaves as “False” when the appliance is in passive monitoring mode.
True	The link on the corresponding inline port will be broken when one of the links is down (such as when a cable is broken or disconnected).
False	The link on the corresponding inline port is left intact when one of the links is down.

9. In the **Adapter Mode (Non HA)** list, select the appliance mode.

   Important: If you change an appliance's monitoring mode from Simulation to Protection, the following Advanced Parameters are enabled by default:

   - np.drop.invalid.checksum
   - np.drop.invalid.protocol

10. Select a **Fail Mode** for the appliance.

    Important: The GX4000 series appliances fail open by default; the GX5000 and GX6000 series appliances fail closed by default. You cannot change these modes.

11. Click **OK**.
12. Save your changes.

Enabling HA

To enable high availability, do the following on *both* appliances:

1. Select **Local Tuning Parameters**.
2. Select the **Adapter Management** tab.

   The Sensor High Availability Mode is located on the bottom half of the page.

3. Select one of the following modes:

   - **HA simulation**
   - **HA protection**

   Note: You must select the same mode on both appliances.

4. Save your changes.

   Note: The adapter modes are pre-set and are not editable when HA mode is enabled. All monitoring adapters are put into inline simulation mode when you select HA simulation mode, or into inline protection mode if you select HA protection mode. The appliances preserve settings for the non-HA adapter modes but do not use them unless you switch them back to normal mode.

Disabling HA

To disable high availability

1. Select **Local Tuning Parameters**.
2. Select the **Adapter Management** tab.

   The Sensor High Availability Mode is located on the bottom half of the page.

3. Select **Normal**.
4. Save your changes.

Managing the Alert Queue

Introduction

The appliance uses a queue file named SensorEventQueue.adf to store event alerts. Use the Alert Queue page to determine how large this file can become before alerts are lost and how the queue file handles alerts after the maximum file size is reached.

Important: If you change any settings on this page, the appliance may lose link temporarily.

Alert queue and SiteProtector

The options you select on this page only change settings for Proventia Manager queue file. When you are managing the appliance through SiteProtector, event data flows directly through a separate queue to the Event Collector and into the Site Database. However, if communication goes down between the appliance and the Event Collector, or between the Event Collector and the Site Database, the event data is stored in a queue file. When normal communication resumes, the queued data is committed through the Event Collector to the Site Database.

Procedure

To manage the alert queue size:

1. Select **Local Tuning Parameters**.
2. Select the **Alert Queue** tab.
3. Complete or change the settings as indicated in the following table.

Setting	Description
Proventia Manager Alert Queue Max Size	Type the maximum size of the alert queue file in bytes.
Proventia Manager Alert Queue Full Policy	Select the method the appliance should use once the queue reaches its maximum size, as follows: • **Stop Logging**. The queue file stops logging alerts when the maximum file size is reached. • **Wrap Around**. The queue file overwrites the oldest alert in order to create space for the new alert, when the maximum file size is reached.

4. Save your changes.

   Important: When you save changes on this page, the agent must restart. This may briefly impact the network and security, as the agent goes into bypass for a short time.

Configuring Advanced Parameters

Introduction

You can use the Advanced Parameters tab to configure (or tune) certain parameters for a specific appliance to better meet your security needs or enhance the performance of the hardware.

You can tune the following components for each appliance:

- intrusion prevention responses
- intrusion prevention security risks
- firewall
- automatic updates

About advanced parameters

Advanced parameters are composed of name/value pairs. Each name/value pair has a default value. For example, the parameter np.firewall.log is a parameter that determines whether to log the details of packets that match firewall rules you have enabled. The default value for this parameter is on.

You can edit the value of any parameter that appears in the list on the Advanced Parameters tab. If the parameter does not appear in the list, it does not mean the parameter has no default value. You simply need to add the parameter to the list with the new value.

For information about update advanced parameters, see. For information about firewall logging parameters, see "Tuning Firewall Logging" on page 120.

Common advanced tuning parameters

The following table describes common advanced tuning parameters:

Name	Type	Default Value	Description
crm.history.enabled	boolean	true	Determines whether to log administrative history.
crm.history.file	string	/var/iss/ crmhistory.log	The administrative history file name.
crm.policy.numbackups	number	4	The number of previous policy files to save.
engine.adapter.high-water.default	number	5	The number of packets per traffic sampling interval that are expected to flow on each adapter. The high-water mark is used to prevent multiple low traffic warnings from being issued when the traffic is hovering around low-water mark.

Table 37: *Common advanced tuning parameters*

Name	Type	Default Value	Description
engine.adapter.low-water.default	number	1	The minimum number of packets per traffic sampling interval that are expected to flow on each adapter. The low-water mark is used as the threshold to issue Network_Quiet and Network_Normal audit events.
engine.droplog.enabled	boolean	false	Determines whether logging of dropped packets is enabled.
engine.droplog.fileprefix	string	/var/iss/drop	The drop log file name prefix.
engine.droplog.filesuffix	string	.enc	The drop log file name suffix.
engine.droplog.flush	boolean	false	Disables buffering of dropped packets. Enabling this adversely affects performance.
engine.droplog.maxfiles	number	10	The number of drop log files to save.
engine.droplog.maxkbytes	number	10000 (kb)	The maximum size of a drop log file.
engine.evidencelog.fileprefix	string	/var/iss/ evidence	The evidence file name prefix.
engine.evidencelog.filesufffix	string	.enc	The evidence file name suffix.
engine.evidencelog.maxfiles	number	10	The number of evidence files to save.
engine.evidencelog.maxkbytes	number	10000 (kb)	The maximum size of an evidence file.
engine.log.file	string	/var/iss/ engine#.log	The engine log file name.
engine.pam.logfile	string	/var/iss/ pam#.log	The PAM log file name.
engine.statistics.interval	number	120	The number of seconds between statistics gathering.
np.drop.invalid.checksum	string	true	Determines whether to block packets with checksum errors in inline protection mode.
np.drop.invalid.protocol	string	true	Determines whether to block packets that violate protocol in inline protection mode.
np.drop.resource.error	string	false	Determines whether to block packets if there are insufficient resources to inspect them in inline protection mode.

Table 37: *Common advanced tuning parameters (Continued)*

Name	Type	Default Value	Description
np.drop.rogue.tcp.packets	string	false	Determines whether to block packets that are not part of a known TCP connection in inline protection mode.
np.firewall.log	string	on	Determines whether to log the details of packets that match firewall rules that are enabled.
np.log.quarantine.added	string	on	Logs the details of rules that are added to the quarantine table.
np.log.quarantine.expired	string	on	Logs the details of rules that have expired from the quarantine table.
np.log.quarantine.removed	string	on	Logs the details of rules that are removed from the quarantine table before they have expired.
np.statistics	string	on	Determines whether logging of PAM statistics is enabled.
np.statistics.file	on	/var/iss/ pamstats.dat	The PAM statistics file name.
pam.traffic.sample	boolean	true	Enables traffic sampling for the purpose of detecting abnormal levels of network activity. This parameter affects the Network_Quiet and Network_Normal audit events.
pam.traffic.sample.interval	number	300	The interval, expressed in seconds, at which traffic flow should be sampled for the purpose of detecting abnormal levels of network activity. This parameter affects the Network_Quiet and Network_Normal audit event.
sensor.trace.level	number	3	The Proventia Network IPS log level.

Table 37: *Common advanced tuning parameters (Continued)*

Adding advanced parameters

To add advanced parameters:

1. Select **Local Tuning Parameters**.
2. Select the **Advanced Parameters** tab.
3. Click **Add**.
4. Complete the settings as indicated in the following table.

Setting	Description
Enabled	Select this check box to enable the parameter.
Name	Type a name for the parameter. **Example**: engine.log.file
Comment	Type a unique description for the parameter. **Example**: The engine log file.
Value	Select one of the following options: • **Boolean**. Select a value of True or False. • **Number**. Enter the appropriate number for the parameter. • **String**. Type the value for the parameter, such a log file location. Example: /var/iss/engine#.log

5. Click **OK**.
6. Save your changes.

Working with advanced parameters

To edit, copy, or remove advanced parameters:

1. Select **Local Tuning Parameters**.
2. Select the **Advanced Parameters** tab, and then do one of the following:

If you want to...	Then...
Edit	**Tip**: You can edit some properties directly on the Advanced Parameters tab by double-clicking the item you want to configure. 1. Select the parameter, and then click the **Edit** icon. 2. Select or clear the **Enabled** check box. 3. Edit the parameter, and then click **OK**.
Copy	1. Select the parameter, and then click the **Copy** icon. 2. Click the **Paste** icon. 3. Edit the parameter as needed, and then click **OK**.
Remove	1. Select the parameter. 2. Click the **Remove** icon.

3. Save your changes.

Configuring TCPReset

Introduction

You can use the appliance to monitor (read-only) SPAN ports on network equipment. To monitor (read-only) SPAN ports, you must configure the appliance's TCPReset (kill) port. If using (read-only) monitoring ports, the appliance must send TCP Resets on another interface.

Note: The appliance is configured by default to send TCP Resets through the monitoring ports even in passive monitoring mode. For example, if you are monitoring through a hub, you do not need to configure the external kill port.

Procedure

To configure TCPReset:

1. Connect the kill port (the Management port labeled 2 on the front of the appliance) to the network.
2. To determine the MAC address of the router of the kill port (eth0), do one of the following:
   - Contact your system administrator to get the MAC address of the router. Once you have received the MAC address, go to Step 4.
   - Run the get-reset-config script on the appliance to get the MAC address. Go to Step 3.
3. Login to the appliance as root and run `get-reset-config`.

   Note the following:
   - If you run the script without parameters, it displays usage information.
   - If you run the script with required parameters, it displays the MAC address.

   Note: The `get-reset-config` utility requires a temporary IP address to connect to the network in order to detect the router's MAC address. During normal operation, the kill port is in stealth mode and does not require an IP address
4. In Proventia Manager, select **System→Local Tuning Parameters**.
5. Select the **Advanced Parameters** tab.
6. Add the local tuning parameter `np.macaddress.destination` to configure the MAC address of the router:

   ```
   np.macaddress.destination = XX:XX:XX:XX:XX:XX
   ```

   Note: See "Adding advanced parameters" on page 132 for more information about adding a local parameter.
7. Select the **Adapter Management** tab.
8. Select the adapter for which you want to enable the External Kill port, and then click **Edit**.
9. On each port where you want to enable the External Kill port, change **TCP Resets** from "This Port" to "TCP Reset Port", and then click **OK**.
10. To enable External Kill ports on other adapters, repeat Steps 8 and 9.

    Example: You can enable the External Kill port to send TCP Resets for events received on ports A, B, C, and D, but you can also choose to send TCP resets for events received on ports E and F through E and F.
11. Click **Save Changes**.

Increasing Maximum Network Frame Size

Introduction

By default, the Proventia Network IPS GX5000 series appliances support a maximum network frame size of 9216 bytes, including the Ethernet FCS (Frame Check Sequence). Ordinary Ethernet (and, in particular, IEEE 802.3 standard) frames are limited to 1518 bytes.

Certain types of network equipment support "jumbo" frames; generally, any frame larger than 1518 bytes is considered a jumbo frame. Most modern network equipment, especially gigabit-capable equipment, now supports jumbo frames, but many equipment types limit the frame size to about 9000 bytes. If the network uses jumbo frames larger than 9216 bytes, you can increase the frame buffer size by setting an advanced tuning parameter.

Important: Increase frame size only if it is absolutely necessary for the network. The amount of memory available to hold network frames is not increased when you increase the maximum frame size. Instead, using larger buffers means that the appliance will be able to hold correspondingly fewer frames at any instant. As a result, the "backlog" of received packets awaiting analysis is shorter, and on very busy networks, the appliance may drop packets if it cannot analyze them quickly enough.

Procedure

To increase the network frame size:

1. Select **Local Tuning Parameters**.
2. Select the **Advanced Parameters** tab.
3. Click **Add**.
4. Complete or change the settings as indicated in the following table.

Setting	Description
Enabled	Select this check box to enable the parameter.
Name	Type *adapter.MaxFrameSize*.
Comment	Type a unique description for the parameter. **Example**: Frame Size Allowance
Value	Select Number, and then enter the appropriate number for the frame size. **Important**: You must enter a number greater than or equal to 1536, and less than or equal to 16384. The number must be a multiple of 512. Otherwise, the value is ignored.

5. Click **OK**.
6. Save your changes.

Chapter 12

Managing System Settings

Overview

Introduction

This chapter explains how to view system status and how to change system settings and properties. Use Proventia Manager to complete the procedures in this chapter. Even if you are managing the appliance through SiteProtector, you must use Proventia Manager to configure these local settings.

In this chapter

This chapter contains the following topics:

Topic	Page
Viewing System Status	136
Managing Log Files	137
Working with System Tools	138
Configuring User Access	139
Installing and Viewing Current Licenses	140

Viewing System Status

Introduction

Review system status information occasionally to ensure the appliance is not overwhelmed by network traffic. System settings can also help you detect any sudden changes in memory or CPU usage.

Procedure

To view system status:

1. In the navigation pane, select **System**.

   The following system information appears:

Table	Statistic	Description
Memory Usage	Total Memory	Amount of memory installed on the appliance.
	Used Memory	Amount of memory currently used by running processes.
	Free Memory	Amount of unused memory on the appliance.
CPU Usage	User	Percentage of CPU resources used by user-level processes.
	System	Percentage of system resources used by the kernel.
	Idle	Percentage of CPU resources currently not used.

2. To refresh the information, select a value from the **Refresh Data** list.

   Tip: Select **Refresh Now** to manually refresh the page.

Managing Log Files

Introduction

The Log Files page in Proventia Manager displays all the log files associated with the appliance. Use this page to view, download, or delete system logs.

About timestamps in log files

Timestamps in some log files are stored in Unix time (the number of seconds elapsed since 00:00:00 on January 1, 1970 UTC). You can use a tool called logtime to translate these timestamps to local time.

Important: You must perform this operation on the appliance itself.

Downloading log files

To download log files:

1. In the navigation pane, select **System→Log Files**.
2. Select a file to download, and then click **Download**.
3. Select **Save the file to disk**, and then click **OK**.
4. Type a **File Name**, and then click **Save**.

   Note: After the download, the saved log file still exists on the appliance.

Translating log file timestamps

To translate the log file timestamps:

1. Log on to the appliance as root.
2. Run logtime with the required parameters. If you run logtime without the arguments, logtime will display usage information.

   Example: To translate timestamps in the firewall log file frw000.log, run the following command:

   ```
   logtime /var/iss/frw000.log /var/iss/newfrw000.log
   ```

   This command creates a new file called newfrw000.log based on the frw000.log file, but the timestamps in the new file are in local time. The original log file is not modified.

   If you create the new translated log file in /var/iss directory, you can download it from Proventia Manager.

Working with System Tools

Introduction

Use the System Tools page to perform basic system tasks, such as the following:

- handling problems with the appliance management port
- testing whether the appliance is communicating correctly with SiteProtector
- testing whether the appliance can communicate with configured SNMP trap receivers, email servers, or NTP servers

Important: You can only perform these tasks in Proventia Manager.

Rebooting the appliance

To reboot the appliance:

1. In Proventia Manager, select **System→Tools**.
2. Click **Reboot**.
3. Click **OK** to reboot the appliance.

Shutting down the appliance

To shut down the appliance:

1. In Proventia Manager, select **System→Tools**.
2. Click **Shut Down**.
3. Click **OK** to shut down the appliance.

Pinging a computer

To ping a computer:

1. In Proventia Manager, select **System→Tools**.
2. In the Diagnostics area, type the IP address of the computer you want to test in the **Ping** box.
3. Click **Submit**.

Using the traceroute utility

To use the traceroute utility:

1. Select **System→Tools**.
2. In the Diagnostics area, type the IP address you want to trace in the **Traceroute** box.
3. Select a **Protocol**, as follows:

Protocol	Description
UDP	When you select a UDP traceroute protocol (UNIX "traceroute" command), the appliance sends a UDP packet to a random port on the target host. The TTL (Time to Live) field and the destination port field are incremented for each "ICMP Port Unreachable" message that is returned, or 30 hops are reached.
ICMP	When you select a ICMP traceroute protocol (Windows "tracert" command), the TTL (Time to Live) field and the destination port field are incremented for each "ICMP Echo Request" message that is returned, or 30 hops are reached.

4. Click **Submit**.

Configuring User Access

Introduction

You can change the following passwords in the Proventia Manager interface:

- root password for the command line
- administrative password for the Proventia appliance
- Web administrative password for Proventia Manager

Important: Record and protect your passwords. If you lose a password, you must reinstall the appliance and reconfigure the network settings.

You can also enable or disable the bootloader (root) password. The bootloader password protects the appliance from unauthorized users during the boot process. When you enable the bootloader password, then you must enter the root password to use a boot option other than the default.

Changing passwords

To change passwords:

1. In Proventia Manager, select **System→ Access**.
2. In the area for the password you want to change, type the **Current Password**.
3. Click **Set Password**.
4. Type the new password twice to confirm it, and then click **OK**.
5. Click **Save Changes**.

Enabling or disabling the bootloader password

To enable the bootloader password:

1. In the navigation pane, select **System→ Access**.
2. Select or clear the **Enable bootloader password** check box, depending on whether you want to enable or disable the password.
3. Click **Save Changes**.

Installing and Viewing Current Licenses

Introduction

The appliance must have a valid license key to apply updates. Use the Licensing page to view important information about the current status of the license file, including expiration dates, and to enter new license key files. Each license key file you install is unique to the product license and may require that you provide IP address range information specific to the network. You can also access the License Information page, which tells you how to acquire a current license.

Important: ISS is bound by its confidentiality policy not to share the network information with any other organization, except as required by law.

Installing a license key file

To install a license key file:

1. In Proventia Manager, select **System→Licensing**.
2. Click **Browse** in the Upload a new License Key box.
3. Locate the license key file that you downloaded.
4. Click **OK**.
5. Click **Upload**.

Viewing current license settings

To view current license settings:

1. In Proventia Manager, select **System→Licensing**.
2. Review the following **Status** information:

Status	Description
Serial Number	The serial number of the license key. **Note**: Each license key has its own serial number, unique to the Identity and the OCN.
OCN	The Order Confirmation Number (OCN) or your customer number with ISS.
Expiration	The date the license expires, in yyyy-mm-dd format.
Maintenance Expiration	The date the maintenance agreement expires, in yyyy-mm-dd format.

3. To access information about acquiring or maintaining licenses, click **License Renewal Information**.

   The License Information page appears and tells you how to contact an ISS representative.

Chapter 13

Viewing Alerts and System Information

Introduction

This chapter describes how to view system alerts, events, logs, and statistics in Proventia Manager.

This chapter contains the following topics:

Topic	Page
Viewing Alerts	142
Managing Saved Alert Files	145
Viewing Notifications Status	146
Viewing Statistics	147

Viewing Alerts

Introduction

Use the Alerts page in Proventia Manager to view and manage system- and security-related alerts. The alerts list contains the following alert types:

- intrusion prevention alerts are related to attempted attacks that occur in the network
- system alerts are related the appliance and its operation

Reference: See "Configuring Alerts" on page 122 for more information about creating alerts to display in the management console.

How the appliance saves the alert list

The current list is saved as three comma separated values (.csv) files. The three files are used to cross-reference the data that appears in the Alerts page. The files are as follows:

This file...	Contains...
filename_eventdata.csv	the distinct records that match the alert record number. This file also lists the alert name and the risk level.
filename_eventinfo.csv	the data listed in the alert specific information section of the alert.
filename_eventresp.csv	the data from the responses executed section of the alert.

Table 38: *Alert list files*

Viewing alert information

To view alert information:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Prevention→Alerts

     System→Alerts

   The Alerts tab displays the following information about each alert:

Column	Description
Rec.#	Record number of the alert.
Risk Level	Risk level icon for the alert.
Alert Name	The alert name.
Source IP	The source IP address of the traffic that caused the alert.
Source Port	The source port and port name of the traffic that caused the alert.
Destination IP	The destination (or target) IP address of the alert.
Destination Port	The destination (or target) port and port name of the alert.
Protocol	The alert's protocol and protocol number.
Vuln Status	The vulnerability status.
Alert Date & Time	The date and time the alert occurred.

2. To view an alert's details, click the **Alert Name**.

   Tip: To view the previous or next alert's details, click the UP or DOWN arrows.

3. To refresh the view, from the **Refresh Data** list, select one of the following:
   - To refresh the list immediately, select **Refresh Now**.
   - To refresh the list automatically, select the time interval.

   Tip: Select **Auto Off** to turn off automatic refresh. If you select this option, you must manually refresh the page to view the latest alerts.

Filtering alerts

To filter alerts:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Prevention→Alerts

     System→Alerts

2. On the Alerts tab, select one of the **Filter Options** listed in the following table:

Option	Description
Risk Level	Displays alerts by the level you select from the **Risk Level** list.
Alert Name	Type the **Alert Name** for which you want to search. You can use wildcard characters to search for alert names.
Alert Type	Select an **Alert Type**, Intrusion Prevention or System.
Date and Time	Enter a specific **Start Date and Time** or **End Date and Time** to search for alerts.
Source IP	Search for alerts for the **Source IP** address you specify.
Target IP	Search for alerts for the **Target IP** address you specify.
Source and Target IP	Search for alerts for both the **Source and Target IP** addresses you specify.
Source Port Number	Search for alerts for the **Source Port Number** you specify.
Target Port Number	Search for alerts for the **Target Port Number** you specify.
Protocol Number	Search for alerts by the **Protocol Number** you specify.
Multiple Values	Enter a combination of filters to search for alerts. For example, you could enter values for Date and Time, Source IP, and Protocol Type to narrow the search.

Saving the alerts list

To save the alerts list:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Prevention→Alerts

     System→Alerts
2. On the Alerts tab, click **Save alerts list to file**.
3. Select the log where you want to save the information, and then click **Download**.
4. On the File Download dialog box, click **Save**.
5. Do one of the following:
   - To save this information in a new file, type the new file name and click **Save**.
   - To save this information in an existing file, click **Save**.

Clearing alerts from the list

To clear alerts from the list:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Prevention→Alerts

     System→Alerts
2. On the Alerts tab, click **Clear alerts list**.
3. Click **OK**.

Managing Saved Alert Files

Introduction

Use the Log File Management page in Proventia Manager to view and manage saved alerts files by either downloading the files to another system, deleting the files, or by doing both. After you download files to another system, the saved file still exists on the appliance.

Downloading alert files

To download alert files:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Prevention→Alerts

     System→Alerts
2. On the Alerts page, click **View/manage alerts files**.
3. Select a file to download, and then click **Download**.
4. Select **Save the file to disk**, and then click **OK**.
5. Type a **File Name**, and then click **Save**.

Deleting alert files

To delete alert files:

1. Do one of the following:
   - Click the **Alerts** button.
   - Select one of the following:

     Notifications→Alerts

     Intrusion Prevention→Alerts

     System→Alerts
2. On the Alerts page, click **View/manage alerts files**.
3. Do one of the following:
   - Select a file to delete, and then click **Delete**.
   - Click **Delete All**.
4. Click **OK**.

Viewing Notifications Status

Introduction

The Notifications Status area provides valuable information about actions taking place on the appliance.

You can view or change the following:

- Alert log event data
- System logs

Viewing alert log event data

Use the Alert Event Log information on the Notifications Status page to monitor the size and number of your event logs. Monitoring this information will help you effectively manage system and event data. If a serious event occurs, you will be able to find the information and solve the problem quickly.

The Alert Event Log table provides the following information:

Item	Description
Number of Logged Alerts	The number of alerts written to the log file.
Percentage Full	The percentage of allocated space that contains alerts log entries.
Time of Last Alert	The date and time of the last alert written to the log file.

Table 39: *Alert log event data*

Viewing system logs

Use the System Logs page to view the system log. System logs contain important information about actions the application has taken, either because a user performed the action (system restart or manual feature configuration), or the appliance has performed the action itself (such as an automatic update).

Refreshing notification status data

You can refresh the page manually or automatically at certain intervals.

To refresh the data:

- Select an option from the **Refresh Data** list:
  - Refresh Now (Use this option to manually refresh the page.)
  - every 10 seconds
  - every 20 seconds
  - every 30 seconds
  - every 1 minute
  - every 2 minutes
  - Auto Off (Use this option to disable automatic refresh.)

  The appliance refreshes the page to display the latest events.

Viewing Statistics

Introduction

Use the Statistics page to view the statistics of network traffic processed by the appliance. You can use these statistics for testing purposes, troubleshooting, or some type of auditing to discover network data and attack trends.

Viewing statistics

To view the statistics:

1. On the Proventia Manager navigation pane, select **Statistics**.
2. Select one of the following statistics pages to view:

Statistic	Description
Protection Statistics	Use the Protection Statistics page to view information about the current appliance configuration and behavior that occurred as a result of the configuration. This information includes statistics about enabled event checks, as well as details about attack and blocking actions the appliance has taken.
Packet Analysis Statistics	Use the Packet Analysis Statistics page to view all the statistics output by the Protocol Analysis Module (PAM). You can use this information to track protocol counts and protocol processing.
Network Statistics	Use the Network Statistics page to view network activity on each adapter used on the appliance, as well as information about packet counts (such as packets injected, rejected, or dropped), or any unanalyzed packets that have passed through the network. Unanalyzed packets can pass through when the appliance is overloaded, or because of routine events such as policy “push” through groups.

Types of driver packets

The following table describes the driver packets:

Packets	Description
Received Packets	The number of packets received since the adapter instance was created.
Transmitted Packets	The number of packets transmitted since the adapter instance was created. This number includes packets forwarded, injected, or unanalyzed.
Forwarded Packets	The number of packets forwarded to a twinned or mirror interface since the adapter instance was created. This number does not include injected packets, but does include packets forwarded without analysis.
Dropped Packets	The number of packets not forwarded (dropped) since the adapter instance was created. (Includes those dropped without analysis.)
Injected Packets	The number of packets injected (i.e. transmitted packets constructed by the application) since the adapter instance was created.

Table 40: *Driver packets*

Packets	Description
Unanalyzed Packets	The number of packets forwarded or dropped without analysis since the adapter instance was created. Unanalyzed packets are processed by the driver whenever the application cannot process them as quickly as they are being received. Whether unanalyzed packets are forwarded or dropped as well as the threshold at which the driver determines that the application is not keeping up is determined by configuration parameters.

Table 40: *Driver packets*

Index

a

adapter clause 117
adapter modes
  inline protection 17
  inline simulation 17
  network adapter cards 127
  passive monitoring 17
  settings 23
admin password 27
advanced parameters
  updates 56
agent
  name 25
  status 25
agent management 25
  agent name 25
  agent status 25
Agent Manager 60, 63
agent name 22, 24
alert queue 128
alerts 122, 142
  alert list 142
  alert queue 128
  error 122
  filters 143
  hardware 122
  informative 122
  log event data 146
  saved files 145
  SNMP 122
  warning 122
appliance
  adapter modes 17
  alerts 142
  documentation 8
  driver packets 147
  firmware reinstallation 28
  information 24
  management 25
  management features 16
  models 7
appliance (cont'd)
  notifications 146
  passwords 22
  ping 138
  protection features 14
  reboot 138
  remote connection 21
  settings checklist 20
  shut down 138
  SiteProtector 60
  statistics 147
  system logs 146
  traceroute utility 138
  updates 50
  user access 139
appliance information
  agent name 24
  base version 24
  firmware version 24
  gateway 25
  host name 24
  IP address 24
  netmask 25
  primary DNS 25
  secondary DNS 25
  serial number 24
  XPU version 24
appliance management 25
  backup 25
  reboot 25
  restore 25
  root access 25
  shut down 25
automatic updates 52

b

backup 25
base version 24
Block response 68
bootloader password 27, 139

c

connection events 93
contexts
  DNS_Query 100
conventions, typographical
  in commands 9
  in procedures 9
  in this manual 9
CPU usage 136

d

date/time 22
DNS
  primary 25
  secondary 25
DNS_Query context 100
documentation 8
driver packets 147
  dropped 147
  forwarded packets 147
  injected 147
  received packets 147
  transmitted packets 147
  unanalyzed 148
driver statistics. See network statistics
dropped packets 147
duplex speed settings 126

e

email responses 69
Email_Receiver context 100
Email_Sender context 101
Email_Subject context 101
ethernet clause 117
events
  connection 93
  SiteProtector 61
  user-defined 97

f

factory default 25
fail mode 127
File_Name context 101
filters
  alerts 143
  connection events 95
  response 86
  security events 84–85
  user-defined events 107
firewall clauses 117
  adapter clause 117
  ethernet clause 117
  IP datagram clause 117
firewall conditions 118
  ICMP conditions 118
  TCP and UDP conditions 118
firewall expressions 118
firewall logging parameters 120
firewall rules 114
  actions 115
  criteria 114
  examples 119
  expressions 118
  firewall clauses 117
  firewall conditions 118
  language 117
  rule order 114, 116
firmware
  reinstallation 28
firmware updates 50
firmware version 24
forwarded packets 147

g

gateway 25
global protection domain 80, 97
global tuning parameters 110

h

HA 34
High availability (HA)
  HA-capable models 34
high availability (HA)
  clustering 34
  deployment 37
  licensing 36
  limitations 36
  modes 18

high availability (HA) (cont'd)
network adapter cards 125, 127
overview 36
primary/secondary configurations 34
SiteProtector management 35
support 34
Home page 47
host configuration 22
host name 24, 26
Hyperterminal 21

i

ICMP conditions 118
ICMP traceroute protocol 138
Ignore response 68
injected packets 147
inline protection
high availability (HA) 18
inline protection mode 17
inline simulation
high availability (HA) 18
inline simulation mode 17
Internet Security Systems
technical support 10
Web site 10
intrusion prevention
connection events 93
global tuning parameters 110
OpenSignature 108
protection domains 78
quarantined intrusions 92
responses 68
security events 77, 80
updates 50
user-defined events 97
X-Force default blocking 112
IP address 24
IP datagram clause 117
IP settings 26
ISS MIB file 73

l

license 46
licenses
current 140
licensing
high availability (HA) 36
local tuning parameters 121
advanced parameters 129
alert queue 128
alerts 122
common 129
firewall logging 120
network adapter cards 125
log evidence response 71
log files 137
timestamps 137
logs
alert event data 146
system 146

m

management port link 26
manual updates 54
maximum network frame size 134
memory usage 136
modes
high availability (HA) 18
inline protection 17
inline simulation 17
passive monitoring 17

n

netmask 25
network adapter card
traffic processes 126
network adapter cards 125
adapter mode (non-HA) 127
duplex speed settings 126
fail mode 127
high availability (HA) mode 127
port speed settings 126
propagate link 126
TCP Resets 125
network cards
PXE boot 28
network configuration 22, 25–26
host name 26
IP settings 26
management port link 26
RS Kill port link 26
TCPReset port link 26
network statistics 147

network time protocol (NTP) 26
News_Group context 102
notifications 146

o

OpenSignature 108
  parser 109
  risks 108
  syntax 108

p

packet analysis statistics 147
parameters
  common tuning 129
  firewall logging 120
  global tuning 110
  local tuning 129
passive monitoring mode 17
Password context 102
password management 27
  admin password 27
  bootloader password 27
  Proventia Manager 27
  root password 27
passwords 22, 139
  admin 27
  bootloader 27, 139
  Proventia Manager 27
  root 27
ping 138
policies
  security 77
port link speed 23
port speed settings 126
primary DNS 25
protection domains 78
  global 80
  security events 83
  user-defined events 97
protection statistics 147
protection status 47
Proventia Manager 42, 47
  Home page 47
  icons 44
  navigation buttons 43
  navigation pane 43
Proventia Manager (cont'd)
  password 27
  protection status 47
  system messages 48
  system status 47
Proventia Setup 21
  agent management 25
  appliance information 24
  appliance management 25
  network configuration 25–26
  password management 27
  settings checklist 20
  SNMP configuration 27
  time configuration 26
PXE boot
  supported network cards 28
PXE boot server 29

q

quarantine responses 72
  Quarantine Intruder 72
  Quarantine Trojan 72
  Quarantine Worm 72
quarantine rules 92
quarantined intrusions 92

r

reboot 25, 138
received packets 147
Recovery CD 28
regular expressions 105
  library 105
  precedence 105
  syntax 105
reinstallation 28
  Recovery CD 28
  requirements 29
  supported network cards 28
remote connection 21
response filters 86
  columns 90
  event attributes 86
  filter 90
  group by 90
  order 86

responses 68
Block 68
email 69
Ignore 68
log evidence 71
quarantine 72
response objects 68
SNM P ISS MIB file 73
SNMP 73
user specified 75
restore 25
rollback 50
root access 25
root password 27
RS Kill 133
port link settings 26

S

secondary DNS 25
security events 77, 80
columns 84
event values 85
filters 84–85
group by 84
protection domains 83
serial number 24
settings
adapter modes 23
agent name 22
appliance information 24
date/time 22
host configuration 22
network configuration 22
port link speed 23
time zone 22
settings checklist 20
shut down 25, 138
SiteProtector
Agent Manager 60, 63
appliance events 61
appliance management 60
high availability (HA) support 35
icons 65
management options 61
navigation 65
policies and settings 65
registration 62
response objects 68
SiteProtector (cont'd)
supported versions 7
updates 61
SNMP
alerts 122
ISS MIB file 73
responses 73
SNMP configuration 27
SNMP daemon 27
SNMP management
trap receivers 27
SNMP responses 73
SNMP_Community context 103
statistics 147
network 147
packet analysis 147
protection 147
status
notifications 146
system 136
system logs 146
system messages 48
system status 47, 136
CPU usage 136
memory usage 136
system tools 138
ping 138
reboot 138
shut down 138
traceroute utility 138

t

TCP and UDP conditions 118
TCP Resets 125
TCPReset 133
port link settings 26
technical support, Internet Security Systems 10
time configuration 26
date and time 26
network time protocol (NTP) 26
time zone 26
time zone 22, 26
traceroute protocol
ICMP 138
UDP 138
traceroute utility 138

traffic processes
  drop 126
  forward 126
transmitted packets 147
trap receivers 27
tuning parameters
  global 110
typographical conventions 9

u

UDP traceroute protocol 138
unanalyzed packets 148
update settings 53
update tools 55
updates 50
  advanced parameters 56
  automatic 52
  available downloads 54
  cumulative 55
  firmware 50
  intrusion prevention 50
  manual 54
  rollback 50
  rollbacks 55
  settings 53
  SiteProtector 61
  Virtual Patch 51
  X-Press Update Server 50
URL_Data context 103
user access 139
user specified responses 75
  executables 75
  shell scripts 75
User_Login_Name context 104
User_Probe_Name context 104
user-defined event contexts 100
  DNS_Query 100
  Email_Receiver context 100
  Email_Sender context 101
  Email_Subject context 101
  File_Name context 101
  News_Group context 102
  Password context 102
  SNMP_Community context 103
  URL_Data context 103
  User_Login_Name context 104
  User_Probe_Name context 104
user-defined events 97
  columns 107
  event contexts 100
  filters 107
  global protection domain 97
  group by 107
  protection domains 97
  regular expressions 105

v

Virtual Patch 51

w

Web site, Internet Security Systems 10

x

X-Force default blocking 112
X-Press Update Server 50
XPU version 24

Internet Security Systems, Inc., an IBM Company
Software License Agreement

BY INSTALLING, ACTIVATING, COPYING OR OTHERWISE USING THIS SOFTWARE PRODUCT, YOU AGREE TO ALL OF THE PROVISIONS OF THIS ISS SOFTWARE LICENSE AGREEMENT ("LICENSE"). EXCEPT AS MAY BE MODIFIED BY AN APPLICABLE LICENSE NOTIFICATION THAT ACCOMPANIES, PRECEDES, OR FOLLOWS THIS LICENSE, AND AS MAY FURTHER BE DEFINED IN THE USER DOCUMENTATION ACCOMPANYING THE SOFTWARE PRODUCT, YOUR RIGHTS AND OBLIGATIONS WITH RESPECT TO THE USE OF THIS SOFTWARE PRODUCT ARE AS SET FORTH BELOW. IF YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL COPIES OF THE SOFTWARE PRODUCT, INCLUDING ANY LICENSE KEYS, TO ISS WITHIN FIFTEEN (15) DAYS OF RECEIPT FOR A FULL REFUND OF ANY PAID LICENSE FEE. IF THE SOFTWARE PRODUCT WAS OBTAINED BY DOWNLOAD, YOU MAY CERTIFY DESTRUCTION OF ALL COPIES AND ANY LICENSE KEYS IN LIEU OF RETURN.

"ISS" is Internet Security Systems, Inc., an IBM Company.

"Software" is the following, including the original and all whole or partial copies: 1) machine-readable instructions and data, 2) components, 3) audio-visual content (such as images, text, recordings, or pictures), 4) related license materials, and 5) license use documents or keys, and documentation.

1. **License** - The Software is provided in object code and is licensed, not sold. Upon your payment of the applicable fees and ISS' delivery to you of the applicable license notification, Internet Security Systems, Inc., an IBM Company ("ISS") grants to you as the only end user ("Licensee") a nonexclusive and nontransferable, limited license for the accompanying Software, for use only on the specific network configuration, for the number and type of devices, and for the time period ("Term") that are specified in ISS' quotation and Licensee's purchase order, as accepted by ISS. If no Term is specified in the applicable ISS quotation or Licensee purchase order, the license shall be deemed perpetual. ISS limits use of Software based upon the number of nodes, users and/or the number and type of devices upon which it may be installed, used, gather data from, or report on, depending upon the specific Software licensed. A device includes any network addressable device connected to Licensee's network, including remotely, including but not limited to personal computers, workstations, servers, routers, hubs and printers. A device may also include ISS hardware (each an "Appliance") delivered with pre-installed Software and the license associated with such shall be a non-exclusive, nontransferable, perpetual (unless otherwise specified in the applicable ISS quotation or Licensee purchase order), limited license to use such pre-installed Software only in conjunction with the ISS hardware with which it is originally supplied. Except as provided in the immediately preceding sentence, Licensee may reproduce, install and use the Software on multiple devices, provided that the total number and type are authorized by ISS. Licensee may make a reasonable number of backup copies of the Software solely for archival and disaster recovery purposes.
   In connection with certain Software products, ISS licenses security content on a subscription basis for a Term. Content subscriptions are licensed pursuant to this License based upon the number of protected nodes or number of users. Security content is regularly updated and includes, but is not limited to, Internet content (URLs) and spam signatures that ISS classifies, security algorithms, checks, decodes, and ISS' related analysis of such information, all of which is owned and copyrighted by ISS and considered ISS confidential information and intellectual property. Security content may only be used in conjunction with the applicable Software in accordance with this License. The use or re-use of such content for commercial purposes is prohibited.
   Licensee's access to the security content is through an Internet update using the Software. In addition, unknown URLs may be automatically forwarded to ISS through the Software, analyzed, classified, entered into ISS' URL database and provided to Licensee as security content updates at regular intervals. ISS' URL database is located at an ISS facility or as a mirrored version on Licensee's premises. Any access by Licensee to the URL database that is not in conformance with this License is prohibited. Upon expiration of the security content subscription Term, unless Licensee renews such content subscription, Licensee shall implement appropriate system configuration modifications to terminate its use of the content subscription. Except for a perpetual license, upon expiration of the license Term, Licensee shall cease using the Software and certify return or destruction of it upon request.
2. **Migration Utilities** - For Software ISS markets or sells as a Migration Utility, the following shall apply. Provided Licensee holds a valid license to the Software to which the Migration Utility relates (the "Original Software"), ISS grants to Licensee as the only end user a nonexclusive and nontransferable, limited license to the Migration Utility and the related documentation ("Migration Utility") for use only in connection with Licensee's migration of the Original Software to the replacement software, as recommended by ISS in the related documentation. The Term of this License is for as long as Licensee holds a valid license to the applicable Original Software. Licensee may reproduce, install and use the Migration Utility on multiple devices in connection with its migration from the Original Software to the replacement software. Licensee shall implement appropriate safeguards and controls to prevent unlicensed use of the Migration Utility. Licensee may make a reasonable number of backup copies of the Migration Utility solely for archival and disaster recovery purposes.
3. **Third-Party Products** - Use of third party product(s) supplied hereunder, if any, will be subject solely to the manufacturer's terms and conditions that will be provided to Licensee upon delivery. ISS will pass any third party product warranties through to Licensee to the extent ISS is authorized to do so. If ISS supplies Licensee with Crystal Decisions Runtime Software, then the following additional terms apply:
   Licensee agrees not to alter, disassemble, decompile, translate, adapt or reverse-engineer the Runtime Software or the report file (.RPT) format, or to use, distribute or integrate the Runtime Software with any general-purpose report writing, data analysis or report delivery product or any other product that performs the same or similar functions as Crystal Decisions' product offerings;
   Licensee agrees not to use the Runtime Software to create for distribution a product that converts the report file (.RPT) format to an alternative report file format used by any general-purpose report writing, data analysis or report delivery product that is not the property of Crystal Decisions;
   Licensee agrees not to use the Runtime Software on a rental or timesharing basis or to operate a service bureau facility for the benefit of third-parties unless Licensee first acquires an Application Service Provider License from Crystal Decisions;
   CRYSTAL DECISIONS AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS, OR IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. CRYSTAL DECISIONS AND ITS SUPPLIERS SHALL HAVE NO LIABILITY WHATSOEVER UNDER THIS AGREEMENT OR IN CONNECTION WITH THE RUNTIME SOFTWARE.
   In this Section 3 "Runtime Software" means the Crystal Reports software and associated documentation supplied by ISS and any updates, additional modules, or additional software provided by Crystal Decisions in connection therewith; it includes Crystal Decisions' Design Tools, Report Application Server and Runtime Software, but does not include any promotional software or other software products provided in the same package, which shall be governed by the online software license agreements included with such promotional software or software product.
4. **Beta License** - If ISS is providing Licensee with the Software, security content and related documentation, and/or an Appliance as a part of an alpha or beta test, the following terms of this Section 4 additionally apply and supersede any conflicting provisions herein or any other license agreement accompanying, contained or embedded in the subject prototype product or any associated documentation. ISS grants to Licensee a nonexclusive, nontransferable, limited license to use the ISS alpha/beta software program, security content, if any, Appliance and any related documentation furnished by ISS ("Beta Products") for Licensee's evaluation and comment (the "Beta License") during the Test Period. ISS' standard test cycle, which may be extended at ISS' discretion, extends for sixty (60) days, commencing on the date of delivery of the Beta Products (the "Test Period"). Upon expiration of the Test Period or termination of the Beta License, Licensee shall, within thirty (30) days, return to ISS or destroy all copies of the beta Software, and shall furnish ISS written confirmation of such return or destruction upon request. If ISS provides Licensee a beta Appliance, Licensee agrees to discontinue use of and return such Appliance to ISS upon ISS' request and direction. If Licensee does not promptly comply with this request, ISS may, in its sole discretion, invoice Licensee in accordance with ISS' current policies.
   Licensee will provide ISS information reasonably requested by ISS regarding Licensee's experiences with the installation and operation of the Beta Products. Licensee agrees that ISS shall have the right to use, in any manner and for any purpose, any information gained as a result of Licensee's use and evaluation of the Beta Products. Such information shall include but not be limited to changes, modifications and corrections to the Beta Products. Licensee grants to ISS a perpetual, royalty-free, non-exclusive, transferable, sublicensable right and license to use, copy, display, perform, make derivative works of and distribute any report, test result, suggestion or other item resulting from Licensee's evaluation of its installation and operation of the Beta Products.
   LICENSEE AGREES NOT TO EXPORT BETA PRODUCTS DESIGNATED BY ISS IN ITS BETA PRODUCT DOCUMENTATION AS NOT YET CLASSIFIED FOR EXPORT TO ANY DESTINATION OTHER THAN THE U.S. AND THOSE COUNTRIES ELIGIBLE FOR EXPORT UNDER THE PROVISIONS OF 15 CFR § 740.17(A) (SUPPLEMENT 3), CURRENTLY CANADA, THE EUROPEAN UNION, AUSTRALIA, JAPAN, NEW ZEALAND, NORWAY, AND SWITZERLAND.
   If Licensee is ever held or deemed to be the owner of any copyright rights in the Beta Products or any changes, modifications or corrections to the Beta Products, then Licensee hereby irrevocably assigns to ISS all such rights, title and interest and agrees to execute all documents necessary to implement and confirm the letter and intent of this Section. Licensee acknowledges and agrees that the Beta Products (including its existence, nature and specific features) constitute Confidential Information as defined in Section 18. Licensee further agrees to treat as Confidential Information all feedback, reports, test results, suggestions, and other items resulting from Licensee's evaluation and testing of the Beta Products as contemplated in this License. With regard to the Beta Products, ISS has no obligation to provide support, maintenance, upgrades, modifications, or new releases. However, ISS agrees to use commercially reasonable efforts to correct errors in the Beta Products and related documentation within a reasonable time, and will provide Licensee with any corrections it makes available to other evaluation participants. The documentation relating to the Beta Products may be in draft form and will, in many cases, be incomplete. Owing to the experimental nature of the Beta Products, Licensee is advised not to rely exclusively on the Beta Products for any reason. LICENSEE AGREES THAT THE BETA PRODUCTS AND RELATED DOCUMENTATION ARE BEING DELIVERED "AS IS" FOR TEST AND EVALUATION PURPOSES ONLY WITHOUT WARRANTIES OR INDEMNITIES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. LICENSEE ACKNOWLEDGES AND AGREES THAT THE BETA PRODUCT MAY CONTAIN DEFECTS, PRODUCE ERRONEOUS AND UNINTENDED RESULTS AND MAY AFFECT DATA NETWORK SERVICES AND OTHER MATERIALS OF LICENSEE. LICENSEE'S USE OF THE BETA PRODUCT IS AT THE SOLE RISK OF LICENSEE. IN NO EVENT WILL ISS BE LIABLE TO LICENSEE OR

ANY OTHER PERSON FOR DAMAGES, DIRECT OR INDIRECT, OF ANY NATURE, OR EXPENSES INCURRED BY LICENSEE. LICENSEE'S SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE BETA PRODUCT LICENSE BY WRITTEN NOTICE TO ISS.

5. **Evaluation License** - If ISS is providing Licensee with the Software, security content and related documentation on an evaluation trial basis at no cost, such license Term is 30 days from installation, unless a longer period is agreed to in writing by ISS. ISS recommends using Software and security content for evaluation in a non-production, test environment. The following terms of this Section 5 additionally apply and supersede any conflicting provisions herein. Licensee agrees to remove or disable the Software and security content from the authorized platform and return the Software, security content and documentation to ISS upon expiration of the evaluation Term unless otherwise agreed by the parties in writing. ISS has no obligation to provide support, maintenance, upgrades, modifications, or new releases to the Software or security content under evaluation. LICENSEE AGREES THAT THE SOFTWARE, SECURITY CONTENT AND RELATED DOCUMENTATION ARE BEING DELIVERED "AS IS" FOR TEST AND EVALUATION PURPOSES ONLY WITHOUT WARRANTIES OR INDEMNITIES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ISS BE LIABLE TO LICENSEE OR ANY OTHER PERSON FOR DAMAGES, DIRECT OR INDIRECT, OF ANY NATURE, OR EXPENSES INCURRED BY LICENSEE. LICENSEE'S SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE EVALUATION LICENSE BY WRITTEN NOTICE TO ISS.
6. **Covenants** - ISS reserves all intellectual property rights in the Software, security content and Beta Products. Licensee agrees: (i) the Software, security content and/or Beta Products is owned by ISS and/or its licensors, and is protected by copyright laws and international treaty provisions; (ii) to take all reasonable precautions to protect the Software, security content or Beta Product from unauthorized access, disclosure, copying or use; (iii) not to modify, adapt, translate, reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software, security content or Beta Product; (iv) not to use ISS trade names or trademarks; (v) to reproduce all of ISS' and its licensors' copyright notices on any copies of the Software, security content or Beta Product; and (vi) not to transfer, lease, assign, sublicense, or distribute the Software, security content or Beta Product or make it available for timesharing, service bureau, managed services offering, or on-line use.
7. **Support and Maintenance** - Depending upon what maintenance programs Licensee has purchased, ISS will provide maintenance, during the period for which Licensee has paid the applicable maintenance fees, in accordance with its prevailing Maintenance and Support Policy that is available at http://documents.iss.net/maintenance_policy.pdf. Any supplemental Software code or related materials that ISS provides to Licensee as part of any support and maintenance service are to be considered part of the Software and are subject to the terms and conditions of this License, unless otherwise specified.
8. **Limited Warranty** - The commencement date of this limited warranty is the date on which ISS provides Licensee with access to the Software. For a period of ninety (90) days after the commencement date or for the Term (whichever is less), ISS warrants that the Software or security content will conform to material operational specifications described in its then current documentation. However, this limited warranty shall not apply unless (i) the Software or security content is installed, implemented, and operated in accordance with all written instructions and documentation supplied by ISS, (ii) Licensee notifies ISS in writing of any nonconformity within the warranty period, and (iii) Licensee has promptly and properly installed all corrections, new versions, and updates made available by ISS to Licensee. Furthermore, this limited warranty shall not apply to nonconformities arising from any of the following: (i) misuse of the Software or security content, (ii) modification of the Software or security content, (iii) failure by Licensee to utilize compatible computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee timely notifies ISS in writing of any such nonconformity, then ISS shall repair or replace the Software or security content or, if ISS determines that repair or replacement is impractical, ISS may terminate the applicable licenses and refund the applicable license fees, as the sole and exclusive remedies of Licensee for such nonconformity. THIS WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. ISS DOES NOT WARRANT THAT THE SOFTWARE OR THE SECURITY CONTENT WILL MEET LICENSEE'S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE OR SECURITY CONTENT WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE OR SECURITY CONTENT ERRORS WILL BE CORRECTED. LICENSEE UNDERSTANDS AND AGREES THAT THE SOFTWARE AND THE SECURITY CONTENT ARE NO GUARANTEE AGAINST UNSOLICITED E-MAILS, UNDESIRABLE INTERNET CONTENT, INTRUSIONS, VIRUSES, TROJAN HORSES, WORMS, TIME BOMBS, CANCELBOTS OR OTHER SIMILAR HARMFUL OR DELETERIOUS PROGRAMMING ROUTINES AFFECTING LICENSEE'S NETWORK, OR THAT ALL SECURITY THREATS AND VULNERABILITIES, UNSOLICITED E-MAILS OR UNDESIRABLE INTERNET CONTENT WILL BE DETECTED OR THAT THE PERFORMANCE OF THE SOFTWARE AND SECURITY CONTENT WILL RENDER LICENSEE'S SYSTEMS INVULNERABLE TO SECURITY BREACHES. THE REMEDIES SET OUT IN THIS SECTION 8 ARE THE SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THIS LIMITED WARRANTY.
9. **Warranty Disclaimer** - EXCEPT FOR THE LIMITED WARRANTY PROVIDED ABOVE, THE SOFTWARE AND SECURITY CONTENT ARE EACH PROVIDED "AS IS" AND ISS HEREBY DISCLAIMS ALL WARRANTIES AND INDEMNITIES, BOTH EXPRESS AND IMPLIED, INCLUDING IMPLIED WARRANTIES RESPECTING MERCHANTABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. LICENSEE EXPRESSLY ACKNOWLEDGES THAT NO REPRESENTATIONS OTHER THAN THOSE CONTAINED IN THIS LICENSE HAVE BEEN MADE REGARDING THE GOODS OR SERVICES TO BE PROVIDED HEREUNDER, AND THAT LICENSEE HAS NOT RELIED ON ANY REPRESENTATION NOT EXPRESSLY SET OUT IN THIS LICENSE.
10. **Limitation of Liability** - Circumstances may arise where, because of a default on ISS' part or other liability, Licensee is entitled to recover damages from ISS. In each such instance, regardless of the basis on which Licensee may be entitled to claim damages from ISS, (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), ISS is liable for no more than 1) damages for bodily injury (including death) and damage to real property and tangible personal property and 2) the amount of any other actual direct damages up to the charges for the Software or security content that is the subject of the claim. This limitation of liability also applies to ISS' licensors and suppliers. It is the maximum for which they and ISS are collectively responsible.
UNDER NO CIRCUMSTANCES IS ISS, ITS LICENSORS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY: LOSS OF, OR DAMAGE TO, DATA; SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO LICENSEE.
11. **Termination** - Licensee may terminate this License at any time by notifying ISS in writing. All rights granted under this License will terminate immediately, without prior written notice from ISS, at the end of the Term of the License, if not perpetual. If Licensee fails to comply with any provisions of this License, ISS may immediately terminate this License if such default has not been cured within ten (10) days following written notice of default to Licensee. Upon termination or expiration of a license for Software, Licensee shall cease all use of such Software, including Software pre-installed on ISS hardware, and destroy all copies of the Software and associated documentation. Termination of this License shall not relieve Licensee of its obligation to pay all fees incurred prior to such termination and shall not limit either party from pursuing any other remedies available to it.
12. **General Provisions** - This License, together with the identification of the Software and/or security content, pricing and payment terms stated in the applicable ISS quotation and Licensee purchase order (if applicable) as accepted by ISS, constitute the entire agreement between the parties respecting its subject matter. Standard and other additional terms or conditions contained in any purchase order or similar document are hereby expressly rejected and shall have no force or effect. If Licensee has not already downloaded the Software, security content and documentation, then it is available for download at http://www.iss.net/download/. All ISS hardware with pre-installed Software and any other products not delivered by download are delivered f.o.b. origin. Both Licensee and ISS consent to the application of the laws of the State of New York to govern, interpret, and enforce all of Licensee's and ISS' rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this License, without regard to conflict of law principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply. Both Licensee and ISS irrevocably waive any right to a jury trial. If any part of this License is found void or unenforceable, it will not affect the validity of the balance of the License, which shall remain valid and enforceable according to its terms. This License may only be modified in writing signed by an authorized officer of ISS.
13. **Notice to United States Government End Users** - Licensee acknowledges that any Software and security content furnished under this License is commercial computer software and any documentation is commercial technical data developed at private expense and is provided with RESTRICTED RIGHTS. Any use, modification, reproduction, display, release, duplication or disclosure of this commercial computer software by the United States Government or its agencies is subject to the terms, conditions and restrictions of this License in accordance with the United States Federal Acquisition Regulations at 48 C.F.R. Section 12.212 and DFAR Subsection 227.7202-3 and Clause 252.227-7015 or applicable subsequent regulations. Contractor/manufacturer is Internet Security Systems, Inc., 6303 Barfield Road, Atlanta, GA 30328, USA.
14. **Export and Import Compliance** - Each party will comply with applicable import and export control laws and regulations, including those of the United States that prohibit or limit export for certain uses or to certain end users. Many ISS Software products include encryption and export outside of the United States or Canada is strictly controlled by U.S. laws and regulations. ISS makes its current export classification information available at http://www.iss.net/export. Please contact ISS' Sourcing and Fulfillment for export questions relating to the Software or security content (fulfillment@iss.net). Licensee understands that the foregoing obligations are U.S. legal requirements and agrees that they shall survive any term or termination of this License.
15. **Authority** - Because the Software is designed to test or monitor the security of computer network systems and may disclose or create problems in the operation of the systems tested, Licensee and the persons acting for Licensee represent and warrant that: (a) they are fully authorized by the Licensee and the owners of the computer network for which the Software is licensed to enter into this License and to obtain and operate the Software in order to test and monitor that computer network; (b) the Licensee and the owners of that computer network understand and accept the risks involved; and (c) the Licensee shall procure and use the Software in accordance with all applicable laws, regulations and rules.
16. **Disclaimers** - Licensee acknowledges that some of the Software and security content is designed to test the security of computer networks and may disclose or create problems in the operation of the systems tested. Licensee further acknowledges that neither the Software nor security content is fault tolerant or designed or intended for use in hazardous environments requiring fail-safe operation, including, but not limited to, aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which the failure of the Software and security content could lead to death or personal

injury, or severe physical or property damage. ISS disclaims any implied warranty of fitness for High Risk Use. Licensee accepts the risk associated with the foregoing disclaimers and hereby waives all rights, remedies, and causes of action against ISS and releases ISS from all liabilities arising therefrom.

17. **Confidentiality** - "Confidential Information" means all information proprietary to a party or its suppliers that is marked as confidential. Each party acknowledges that during the term of this Agreement, it will be exposed to Confidential Information of the other party. The obligations of the party ("Receiving Party") which receives Confidential Information of the other party ("Disclosing Party") with respect to any particular portion of the Disclosing Party's Confidential Information shall not attach or shall terminate when any of the following occurs: (i) it was in the public domain or generally available to the public at the time of disclosure to the Receiving Party, (ii) it entered the public domain or became generally available to the public through no fault of the Receiving Party subsequent to the time of disclosure to the Receiving Party, (iii) it was or is furnished to the Receiving Party by a third party having the right to furnish it with no obligation of confidentiality to the Disclosing Party, or (iv) it was independently developed by the Receiving Party by individuals not having access to the Confidential Information of the Disclosing Party. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation of this License and to use Confidential Information of the Disclosing Party solely for the purposes of this License. Upon demand by the Disclosing Party and, in any event, upon expiration or termination of this License, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party's Confidential Information in the Receiving Party's possession or control and destroy all derivatives and other vestiges of the Disclosing Party's Confidential Information obtained or created by the Disclosing Party. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party, provided however that the Receiving Party may use in its business activities the ideas, concepts and know-how contained in the Disclosing Party's Confidential Information which are retained in the memories of the Receiving Party's employees who have had access to the Confidential Information under this License.
18. **Compliance** - From time to time, ISS may request Licensee to provide a certification that the Software and security content is being used in accordance with the terms of this License. If so requested, Licensee shall verify its compliance and deliver its certification within forty-five (45) days of the request. The certification shall state Licensee's compliance or non-compliance, including the extent of any non-compliance. ISS may also, at any time, upon thirty (30) days prior written notice, at its own expense appoint a nationally recognized software use auditor, to whom Licensee has no reasonable objection, to audit and examine use and records at Licensee offices during normal business hours, solely for the purpose of confirming that Licensee's use of the Software and security content is in compliance with the terms of this License. ISS will use commercially reasonable efforts to have such audit conducted in a manner such that it will not unreasonably interfere with the normal business operations of Licensee. If such audit should reveal that use of the Software or security content has been expanded beyond the scope of use and/or the number of authorized devices or Licensee certifies such non-compliance, ISS shall have the right to charge Licensee the applicable current list prices required to bring Licensee in compliance with its obligations hereunder with respect to its current use of the Software and security content. In addition to the foregoing, ISS may pursue any other rights and remedies it may have at law, in equity or under this License.
19. **Data Protection** - Licensee confirms that it is solely responsible for ensuring that any processing and security obligations comply with applicable data protection laws. Licensee contact information shall not be considered personal information processed on Licensee's behalf.
20. **Miscellaneous** - Except for any payment obligations, neither Licensee nor ISS is responsible for failure to fulfill any obligations due to causes beyond its control. This License will not create any right or cause of action for any third party, nor will ISS be responsible for any third party claims against Licensee except, as permitted by the Limitation of Liability section above, for bodily injury (including death) or damage to real or tangible personal property for which ISS is legally liable. Nothing in this License affects any statutory rights of consumers that cannot be waived or limited by contract. Licensee agrees to allow ISS to store and use Licensee's contact information, including names, phone numbers, and e-mail addresses, anywhere they do business. Such information will be processed and used in connection with our business relationship, and may be provided to contractors, Business Partners, and assignees of ISS for uses consistent with their collective business activities, including communicating with Licensee (for example, for processing orders, for promotions, and for market research). Neither Licensee nor ISS will bring a legal action under this License more than two years after the cause of action arose unless otherwise provided by local law without the possibility of contractual waiver or limitation.

Revised: February 14, 2007